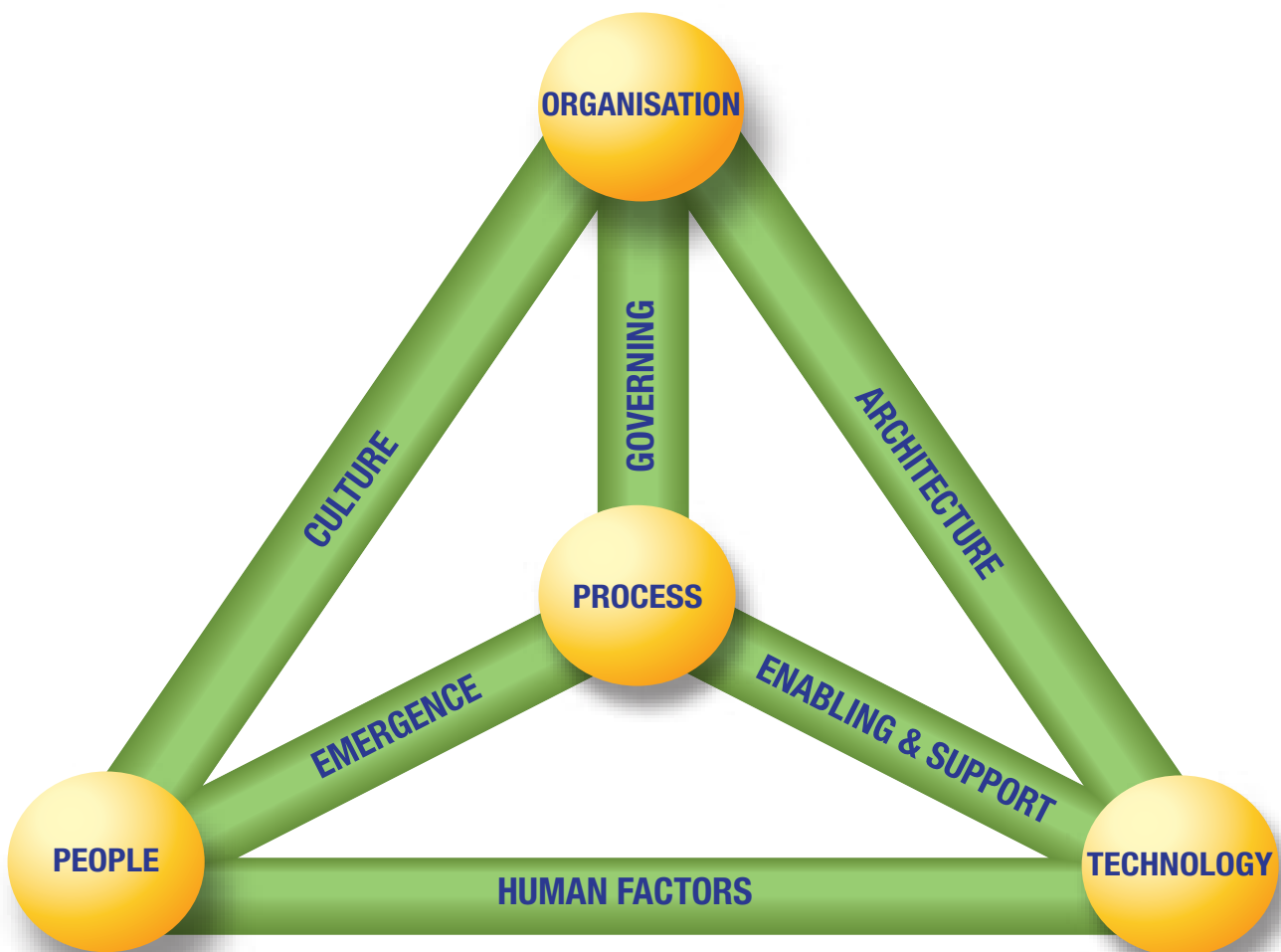


# The Business Model for Information Security



# THE BUSINESS MODEL FOR INFORMATION SECURITY

## ISACA®

With 95,000 constituents in 160 countries, ISACA ([www.isaca.org](http://www.isaca.org)) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the non-profit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor™ (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations. ISACA continually updates COBIT®, which helps IT professionals and enterprise leaders fulfil their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

## Disclaimer

ISACA has designed and created *The Business Model for Information Security* (the ‘Work’) primarily as an educational resource for security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, readers should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

## Reservation of Rights

© 2010 ISACA. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and non-commercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

## ISACA

3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [info@isaca.org](mailto:info@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)

ISBN 978-1-60420-154-3

*The Business Model for Information Security*

Printed in the United States of America

CRISC is a trademark/service mark of ISACA. The mark has been applied for or registered in countries throughout the world.

## ACKNOWLEDGEMENTS

**Author**

Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany

**Development Team**

Derek J. Oliver, Ph.D., DBA, CISA, CISM, CITP, FBCS, FISM, MInstISP, Ravenswood Consulting Ltd., UK  
 Jean-Luc Allard, CISA, CISM, MISIS scri, Belgium  
 Elisabeth Antonsson, CISM, Nordea Bank, Sweden  
 Sanjay Bahl, CISM, Microsoft Corp. Pvt. Ltd., India  
 Krag Brotby, CISM, CGEIT, Brotby & Associates, USA  
 Christos K. Dimitriadis, Ph.D., CISA, CISM, INTRALOT S.A., Greece  
 Meenu Gupta, CISA, CISM, CIPP, CISSP, Mittal Technologies, USA  
 Cristina Ledesma, CISA, CISM, Citibank NA Sucursal, Uruguay

**Expert Reviewers**

Manuel Aceves, CISA, CISM, CISSP, Cerberian Consulting, Mexico  
 Sanjay Bahl, CISM, Microsoft Corp. Pvt. Ltd., India  
 Krag Brotby, CISM, CGEIT, Brotby & Associates, USA  
 Christos K. Dimitriadis, Ph.D., CISA, CISM, INTRALOT S.A., Greece  
 Meenu Gupta, CISA, CISM, CIPP, CISSP, Mittal Technologies, USA  
 Yves LeRoux, CISM, CA Technologies, France  
 Mark A. Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA  
 Derek J. Oliver, Ph.D., DBA, CISA, CISM, CITP, FBCS, FISM, MInstISP, Ravenswood Consulting Ltd., UK  
 Vernon Richard Poole, CISM, CGEIT, Sapphire, UK  
 Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, RSM Bird Cameron, Australia

**ISACA Board of Directors**

Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA, International President  
 Christos K. Dimitriadis, Ph.D., CISA, CISM, INTRALOT S.A., Greece, Vice President  
 Ria Lucas, CISA, CGEIT, Telstra Corp. Ltd., Australia, Vice President  
 Hitoshi Ota, CISA, CISM, CGEIT, CIA, Mizuho Corporate Bank Ltd., Japan, Vice President  
 Jose Angel Pena Ibarra, CGEIT, Alintec S.A., Mexico, Vice President  
 Robert E. Stroud, CGEIT, CA Technologies, USA, Vice President  
 Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President  
 Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany, Vice President  
 Lynn C. Lawton, CISA, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President  
 Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President  
 Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Director  
 Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Director  
 Howard Nicholson, CISA, CGEIT, CRISC, City of Salisbury, Australia, Director  
 Jeff Spivey, CPP, PSP, Security Risk Management, USA, ITGI Trustee

**Framework Committee**

Patrick Stachtchenko, CISA, CGEIT, CA, Stachtchenko & Associates SAS, France, Chair  
 Steven A. Babb, CGEIT, KPMG, UK  
 Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore  
 Sergio Fleginsky, CISA, Akzonobel, Uruguay  
 John W. Lainhart IV, CISA, CISM, CGEIT, IBM Global Business Services, USA  
 Mario C. Micallef, CGEIT, CPAA, FIA, Ganado & Associates, Malta  
 Derek J. Oliver, Ph.D., DBA, CISA, CISM, CITP, FBCS, FISM, MInstISP, Ravenswood Consulting Ltd., UK  
 Robert G. Parker, CISA, CA, CMC, FCA, Canada  
 Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, RSM Bird Cameron, Australia  
 Robert E. Stroud, CGEIT, CA Technologies, USA  
 Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany

## ACKNOWLEDGEMENTS (*CONT.*)

### **Special Recognition**

To the following members of the 2008-2009 Security Management Committee who initiated the project and steered it to a successful conclusion:

Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, RSM Bird Cameron, Australia  
Manuel Aceves, CISA, CISM, CISSP, Cerberian Consulting, Mexico  
Kent Anderson, CISM, Encurve LLC, USA  
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd., USA  
Yves LeRoux, CISM, CA Technologies, France  
Mark A. Lobel, CISA, CISM, CISSP, PricewaterhouseCoopers LLP, USA  
Kyeong Hee-Oh, CISA, CISM, Fullbitsoft, Korea  
Vernon Richard Poole, CISM, CGEIT, Sapphire, UK  
Rolf M. von Roessing, CISA, CISM, CGEIT, Forfa AG, Germany

### **In Recognition**

The Business Model for Information Security is based on research conducted by the University of Southern California Marshall School of Business Institute for Critical Information Infrastructure Protection. ISACA wishes to recognise the contribution to the information security community that was made by Charles P. Meister, Morley Winograd, Phil Cashia, Dr. Ann Majchrzak, Dr. Ian Mitroff, Prof. Dan O'Leary, Dr. Laree Kiely, Terry Benzel, Steve Raynor and Bill Belgard, the authors of the Systemic Security Management Model.

### **ISACA/IT Governance Institute Affiliates and Sponsors**

American Institute of Certified Public Accountants  
ASIS International  
The Center for Internet Security  
Commonwealth Association for Corporate Governance Inc.  
FIDA Inform  
Information Security Forum  
Information Systems Security Association  
Institut de la Gouvernance des Systèmes d'Information  
Institute of Management Accountants Inc.  
ISACA chapters  
ITGI Japan  
Norwich University  
Solvay Brussels School of Economics and Management  
University of Antwerp Management School  
Aldion Consulting Pte. Ltd.  
Analytix Holdings Pty. Ltd.  
B Wise B.V.  
Hewlett-Packard  
ITpreneurs Nederlands B.V.  
Phoenix Business and Systems Process Inc.  
Project Rx Inc.  
SOAProjects Inc.  
Symantec Corp.  
TruArx Inc.  
Wolcott Group LLC  
World Pass IT Solutions

## TABLE OF CONTENTS

<b>Executive Summary .....</b>	<b>7</b>
<b>1. Introduction .....</b>	<b>9</b>
Models .....	10
Frameworks .....	10
Standards .....	11
Combining Models, Frameworks and Standards.....	11
State of Security .....	11
Outcomes of Information Security .....	12
<b>2. Business Model for Information Security .....</b>	<b>13</b>
BMIS Elements .....	14
Organisation.....	14
Process.....	17
Technology .....	20
People.....	23
BMIS Dynamic Interconnections .....	25
Governing .....	25
Culture.....	27
Architecture .....	32
Enabling and Support .....	35
Emergence .....	41
Human Factors .....	43
<b>3. Using BMIS.....</b>	<b>47</b>
Taking Stock: Analysing the Existing Security Programme.....	47
Laws and Regulations.....	48
Enterprise Governance.....	49
Security Compliance.....	49
Other Components of the Security Programme .....	49
Populating BMIS: Existing Security Measures and Solutions.....	50
Gathering Information .....	50
Integrating Individual Solutions .....	50
Integrating Managed Solutions.....	54
Aligning Standards and Frameworks to BMIS .....	55
Information Security Management.....	55
General IT Management.....	57
BMIS Diagnostics: Identifying Strengths and Weaknesses .....	57
Situational Analysis .....	58
Root-cause Analysis.....	59
Setting BMIS in Motion: Improvement Journey.....	62
Converting Security Processes Into Security Subsystems.....	63
Actions and Improvement Steps .....	64
Leveraging System Dynamics .....	67
Conclusion .....	69
<b>ISACA Professional Guidance Publications .....</b>	<b>71</b>

**Page intentionally left blank**

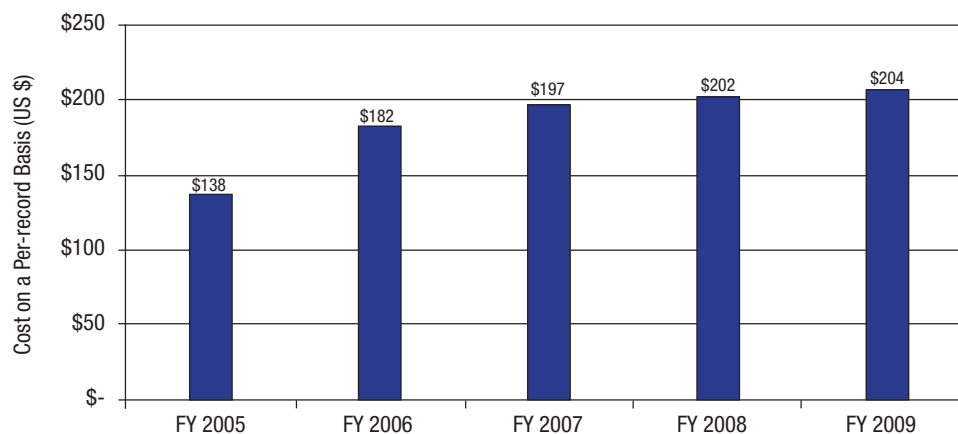
## EXECUTIVE SUMMARY

Information security has become a critical business function. The success of an enterprise is closely affiliated with its ability to manage risks appropriately. Protecting valued and sensitive information has become essential for enterprise sustainability. Effective management of information risks and exposures—as well as opportunities—can directly affect the profitability and overall value of an enterprise.

For too long, information security has been operating in a reactive mode. Security professionals have been reacting to threats, risks, legislation, breaches, emergent technologies and cultural issues and have found themselves in the unfortunate situation of belonging to a relatively young profession that lacks both research and resources to help improve security programmes. These professionals have been forced to comply with piecemeal standards and frameworks to address concerns relating to compliance, privacy and risk, leaving little time for value creation and innovation.

This reactionary mode of managing security has proven ineffective. The information security climate is almost the same as it was 10 years ago. While security controls have increased, so have the number of breaches and their associated costs. The Ponemon Institute issues an annual survey on the cost of a data breach, showing how costs have increased over time<sup>1</sup> (figure 1).

Figure 1—The Rising Cost of Security Breaches



Source: Ponemon Institute, '2009 Annual Study: Cost of a Data Breach—Understanding Financial Impact, Customer Turnover, and Preventive Solutions', figure 1: Average Per-record Cost of a Data Breach 2005-2009, USA, 2010, [http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US\\_Ponemon\\_CODB\\_09\\_012209\\_sec.pdf](http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf)

As security professionals struggle to balance protection with entrepreneurial risk taking in a complex, evolving landscape it has become clear that the current method of controlling risk has proven inadequate and there is a gap between the management of information assets and the people who use them. Current security frameworks do not address issues such as culture, human factors and rapid change. Security professionals need a more effective method to manage enterprise information assets.

Information security has become the business unit responsible for the most important asset an enterprise holds: its corporate information. While the transmission, integrity and availability of that information are critical in conducting global business, its protection is equally important.

The Business Model for Information Security (BMIS) presents a holistic, dynamic solution for designing, implementing and managing information security. As an alternative to applying controls to apparent security symptoms in a cause-and-effect pattern, BMIS examines the entire enterprise system, allowing management to address the true source(s) of problems while maximising elements of the system that can most benefit the enterprise.

By studying all factors that introduce uncertainty and correlating all factors for understanding actual organisational needs, BMIS complements any framework or standard already in place. It will assist enterprises in effectively managing information risk to minimise threats and ensure confidentiality, integrity and availability of information assets while harnessing enterprise information assets to create value.

**The Business Model for Information Security (BMIS) presents a holistic, dynamic solution for designing, implementing and managing information security.**

<sup>1</sup> Ponemon Institute, 'Cost of a Data Breach', USA, 2010, [www.ponemon.org/data-security](http://www.ponemon.org/data-security)

**Page intentionally left blank**



## 1. INTRODUCTION

In January 2009, ISACA introduced the security community to the Business Model for Information Security. The publication<sup>2</sup> offered security professionals a look into a new approach for effective management of information security. BMIS focuses on the business environment within which information security operates amongst other business processes. This particular focus provides a broader view of value-driving processes and systems within the enterprise that impact or are impacted by information security.

As a relatively young profession, information security has struggled to meet business objectives in a rapidly changing risk environment. Although security professionals have managed to keep many potential attacks at bay, there have been several well-publicised, costly security breaches that have caused some to wonder just how effective information security programmes are. From a business perspective, the primary objectives of any enterprise are often far removed from the technical world of IT and information security. To bridge the gap between what the enterprise does and how this is supported by strong security, BMIS realigns technical content with business thinking and a strategic point of view.

To be fair, information security professionals have done a commendable job given the few resources available. Low budgets, limited staffing and restricted access to executive support are common hurdles that information security professionals face while trying to protect information assets, minimise risks and deliver value to the business. Add to this a continuously changing regulatory environment and constantly emerging new risks and it is easy to see why information security has struggled to survive as a function. These obstacles in day-to-day security work often arise out of a fundamental misunderstanding. Although organisational leaders are aware of risks and willing to address risks in a hands-on manner, the complexity of information security requires specific skills and knowledge. More often than not, security experts find it difficult to articulate the value that information security can bring to the business through ensuring that information resources are not only protected from those who should not have access to them, but also that information is available and accurate for those who should have access. BMIS provides the frame and mindset to structure communications amongst senior management and security professionals.

Awareness of the need for information security has grown remarkably, possibly due to increases in both regulation and malicious activity. As a result, some enterprises have created security programmes, placing IT people—some of whom may have had little security experience—in charge of the new initiative. In other enterprises, security professionals have been brought in specifically to resolve existing problems. Other enterprises have used external consultants to design, implement and improve their information security programmes. These initiatives, while positive in themselves, need a larger framework to bring them in line with business objectives. Both security spending and working on specific security measures require a clear business case that can be substantiated at any time to senior management.

Until now there has been no holistic or dynamic model for security managers to use as guidance. There are many standards that can be used for benchmarking and providing direction, and there are just as many frameworks that can serve as useful guides for implementation, but there has been no overarching model that could exist in any enterprise regardless of geographic location, industry, size, regulation or existing protocol.

Many people may think that they are on the right path because they have aligned their programme with an existing standard or framework. While these avenues may seem to lead the security professional in the right direction, there is one essential component missing. Frameworks and standards have helped to address specific needs, but they have not provided a holistic solution that examines the entire enterprise and studies how the organisational mission affects the security programme and *vice versa*. To understand the big picture, information security managers must take a broader view.

BMIS fills this gap and addresses the security programme at the strategic or business level. The model allows security managers to gain a broad view of what is happening in the enterprise, enabling them to better treat information risk while assisting senior management in meeting its goals. By looking at the security programme from a systems perspective, BMIS provides a means for security professionals to consider areas that may not have been accounted for in existing standards. BMIS also provides a mechanism for security professionals to internalise the fact that new threats and new attacks come up regularly.

To understand the model, it is important to distinguish amongst models, standards and frameworks. While BMIS can help overcome some of the known difficulties in information security, it is primarily a model that must be supported by additional standards and frameworks.

---

<sup>2</sup> ISACA, *An Introduction to the Business Model for Information Security*, USA, 2009

# THE BUSINESS MODEL FOR INFORMATION SECURITY

## Models

While there are many definitions for the word ‘model’, they all describe imitation or representation in one way or another. One definition often used for theoretical models is ‘A schematic description of a system, theory or phenomenon that accounts for its known or inferred properties and may be used for further study of its characteristics’.<sup>3</sup> A model can be thought of as a theoretical description of the way a system works. However, it often needs to be simplified to some extent to be useful in practice.

In general, models need to be flexible to meet the needs of the business world. They need to be tested at times to ensure that they are still applicable and fit the intended purpose, and they should incorporate changes in systems and the enterprises in which they exist. It is important to remember that models are descriptive, but not normative. An overarching security model such as BMIS must, therefore, be the foundation for all standards and frameworks applied in the information security arena. At the same time, BMIS must be able to accommodate changes quickly and highlight the consequences to the enterprise.

Models are often used by enterprises to foster innovation and maximise the value generated through innovation or change. They can be used within an enterprise to translate strategy and mission into concepts and steps applying to processes or organisational entities. Models can help define a goal and create the plan for how to get there. Enterprises such as IBM, Xerox and Fujitsu have utilised models for years to improve value chains. In fact, in a business plan the model may be more profitable for the enterprise than the technology itself. An example is the operating plan for the Xerox 914 copier. Xerox had created new technology that was superior to other copy products, but was six to seven times more expensive than the competition. After being turned down by large companies for marketing partnerships, Xerox decided to market the technology itself with a new business model. Instead of selling products

and relying on service for profits, Xerox leased the equipment to customers and then charged a per-copy fee for anything over 2,000 copies. Because the quality that Xerox technology brought to the field was so superior to that of its competition, customers increased the number of copies they made—resulting in a 12-year annual growth rate of 41 percent for the enterprise.

---

**BMIS creates opportunities for the information security programme to establish itself as a solid business enabler by considering security’s impact on the business.**

---

Just as the business model boosted Xerox by extracting economic value for the enterprise through innovative technology, BMIS creates opportunities for the information security programme to establish itself as a solid business enabler by considering security’s impact on the business.

## Frameworks

Frameworks provide structure. They can be thought of as the skeletal system upon which the body of a sound programme can be built. Generally, frameworks are operational in nature and provide a detailed description of how to implement, create or manage a programme or process. Frameworks are typically principles-based and open to continuous improvement. As a result, frameworks usually rely on subsidiary standards to ‘make it happen’, and they are further complemented by implementation guides and other detailed documents.

Frameworks are indispensable tools that can assist security managers in developing and implementing a robust security programme and ensuring its continued success via monitoring. Frameworks are very detailed and provide specific recommended actions that have proven useful for many security managers building a programme. Although there are no frameworks dedicated to information security at this time, there are many risk frameworks that may be of use. OCTAVE<sup>4</sup> is a risk framework. COBIT<sup>5</sup> and the *Internal Control—Integrated Framework*<sup>6</sup> are examples of powerful frameworks covering the governance and management of IT that can be of help when creating and maintaining a security programme. ITIL<sup>7</sup> also defines a security management process based on the code of practice defined in ISO 27002. Additionally, ISACA’s Risk IT framework<sup>8</sup> is a comprehensive framework for managing IT-related risk. In contrast to models discussed previously, frameworks are usually normative rather than descriptive.

---

<sup>3</sup> *American Heritage Dictionary*, USA, 2003

<sup>4</sup> Operationally Critical Threat, Asset, and Vulnerability Evaluation<sup>SM</sup> is a suite of tools, techniques and methods for risk-based information security strategic assessment and planning developed and maintained by the Software Engineering Institute, Carnegie Mellon University, USA.

<sup>5</sup> COBIT 4.1 is the current version developed and maintained by ISACA, USA.

<sup>6</sup> Developed and maintained by the Committee of Sponsoring Organizations (COSO), USA

<sup>7</sup> Information Technology and Infrastructure Library, developed and maintained by the Office of Government Commerce (OGC), UK

<sup>8</sup> ISACA, *The Risk IT Framework*, USA, 2009

## Standards

According to the British Standards Institute (BSI), a standard is an ‘agreed, repeatable way of doing something. It is a published document that contains technical specifications or other precise criteria designed to be used consistently as a rule, guideline, or definition’.<sup>9</sup> An additional definition indicates that a standard is a basis for comparison; a reference point against which other things can be evaluated.<sup>10</sup>

These definitions align with how standards are seen in the information security community: providing information security professionals with a sense of direction and a way of benchmarking an enterprise’s progress towards best practices.

Standards most commonly used in the information security arena include the International Organization for Standardization (ISO) 27001:2005 and the wider ISO 27000 series, the National Institute for Standards and Technology (NIST) Special Publication (SP) 800-53 and the Payment Card Industry Data Security Standard (PCI DSS). The latter is an example of specific information security required for some of the processes that a financial services organisation may be using. However, it often requires further context to enable and inform a cost-effective, integrated implementation of PCI DSS. BMIS can assist in providing the systemic context in which payment card processes are operating, and the consequences for information security steps taken to address the standard.

## Combining Models, Frameworks and Standards

Noting the distinction amongst models, standards and frameworks, it is clear which of the three information security has been missing. Security professionals have long been trying to align programme activities with multiple standards, regulations and frameworks and have been missing an overarching model that would assist them in keeping information protected. Why is a model needed? Even with the use of frameworks and standards, security professionals face challenges such as senior management’s understanding of and commitment to information security initiatives, the involvement of information security in planning prior to the implementation of new technologies, integration between business and information security, alignment of information security with the enterprise’s objectives, and executive and line management ownership and accountability for implementing, monitoring and reporting on information security.

BMIS addresses these challenges by offering a way for enterprises to synthesise the frameworks and standards they are utilising and a formal model they can follow to create a holistic information security programme that does more for the enterprise than traditional approaches.

## State of Security

Changes in technology, global networking and pervasive use of information technology have elevated the need for effective information risk management. As enterprises struggle to remain profitable, executives have recognised that information security breaches can be a serious threat to the brand and image of the enterprise. Information security professionals are in a unique situation: they have become responsible for one of the enterprise’s most important assets and can demonstrate value to the enterprise by aligning the security programme with enterprise objectives and managing the risk to information assets.

In the last 10 years, numerous issues have occurred that affect information security. Among these are regulations such as Basel II, the US Health Insurance Portability and Accountability Act (HIPAA) and the US Sarbanes-Oxley Act; increased insider threats; emergent technologies; and increased external threats. In response, information protection has not improved, at least statistically speaking. In 2005, a group of people began collecting data on security breaches in the United States and posting them online at [www.privacyrights.org](http://www.privacyrights.org). With few exceptions, the statistics demonstrate an alarming pattern of increased data loss. Each year, from 2005 through 2008, the number of data breaches increased: 157 in 2005, 321 in 2006, 446 in 2007 and 656 in 2008.<sup>11</sup> The cost that enterprises are incurring due to these breaches is also escalating.

As mentioned in the Executive Summary and in **figure 1**, the Ponemon Institute conducts an annual study on the cost of security breaches. The cost has increased consistently over the past five years. In 2005 the study revealed that the average cost (direct and indirect costs) to an enterprise was approximately US \$138 per incident. The 2010 results show that in 2009, that cost had risen to approximately US \$204 per incident.<sup>12</sup>

This increase in both cost and frequency of breaches is significant because, during that same period, information security has experienced significant breakthroughs. Technologies such as firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), data leak prevention, end point control, routers, switches and other components such as identity and access

<sup>9</sup> British Standards Institute, *What Is a Standard?*, UK, 2010

<sup>10</sup> Government Statistical Service, *National Statisticians Guidance: Quality, Methods and Harmonisation*, UK, 2009

<sup>11</sup> The Privacy Rights Clearinghouse, USA, 2009

<sup>12</sup> Ponemon Institute, op. cit.

management (IAM) have been created or improved to enable better security. Legislation has increased exponentially, bringing attention to information assets. Crime, terrorism and natural disasters have highlighted the need for improved information protection. The powerful combination of technical innovation, increased awareness from executives and increased resources has been paralleled by increased threats, risks and successful breaches. Security simply has not shown the improvement that would be expected to correlate with the growth the profession has experienced.

One would think that, with the introduction of advanced security technology, increased regulatory focus, and incentives for business to invest in the protection of information, security incidents would be rare. However, the truth is that even with the advances being made, security incidents still happen. Private information is still compromised. Internal incidents and fraud are reported all too frequently. Why is information security not improving in leaps and bounds? One answer is that information security professionals continue to find themselves reacting to issues within the enterprise rather than taking a proactive stance. This constant firefighting leaves little time for innovation, strategic thinking and planning. Security professionals revert to applying controls to problems as they arise, often with an overreliance on technology. This is often accompanied by a lack of historical data, so problems continue to occur, even though they have been ‘fixed’ at some previous point. Another answer is that attacks, negligent behaviour and human error have become more frequent, given the increased use of IT as a way of doing business. A third answer is that the use of IT in day-to-day life has become ubiquitous. Most of our daily activities, from home banking to ordering a pizza, are performed online. Naturally, this creates many new threats and security challenges.

**When information risk management is not integrated into the business, organisational silos can reduce opportunities for strategic solutions.**

Additionally, many enterprise cultures have not accepted information security, and information security managers continue to struggle to demonstrate value. When information risk management is not integrated into the business, organisational silos can reduce opportunities for strategic solutions. A holistic risk-based approach to managing information assets must be implemented. Information security professionals must look at enterprise systems and develop solutions that create opportunities while minimising risk.

## Outcomes of Information Security

Information security needs to be many things to the enterprise. It is the gatekeeper of the enterprise’s information assets. That calls for the information security programme to protect organisational data while also enabling the enterprise to pursue its business objectives—and to tolerate an acceptable level of risk in doing so.

This tension between entrepreneurial risk and protection can be difficult to manage, but it is a critical part of a security professional’s job. Providing information to those who should have it is as significant as protecting it from those who should not have it. Security must enable the business and support its objectives rather than becoming self-serving.

From a governance perspective there are six major outcomes that the security programme should work to achieve. In its publication on information security governance,<sup>13</sup> ISACA defined these outcomes as:

- Strategic alignment
- Risk management
- Value delivery
- Resource management
- Performance management
- Assurance process integration

There are a number of indicators for integration of diverse security-related functions. Most important, there should be no gaps in the level of information asset protection. Overlaps in areas of security planning or management should be minimised. Another indicator is the level of integration for information assurance activities with security. Roles and responsibilities should be clearly defined for specific functions. This includes the relationships between various internal and external providers of information assurance. All assurance functions should be identified and considered in the overall organisational strategy.<sup>14</sup>

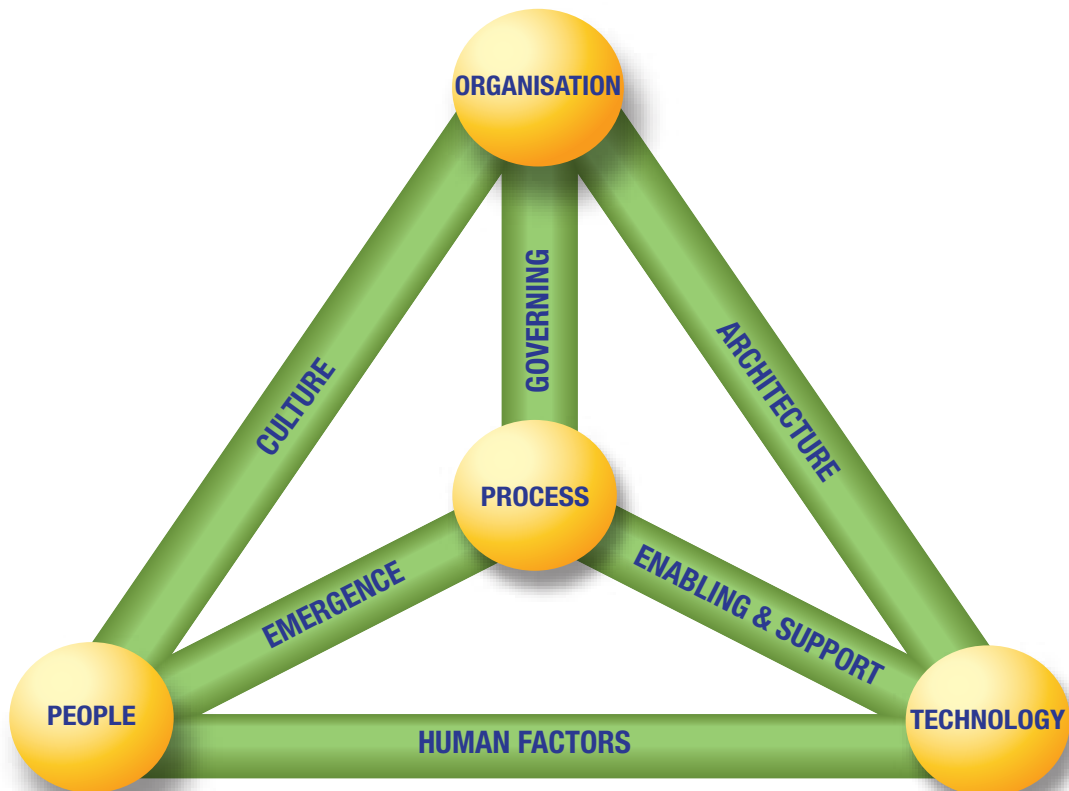
<sup>13</sup> ISACA, *Information Security Governance: Guidance for Information Security Managers*, 2008, USA

<sup>14</sup> Ibid.

### 2. BUSINESS MODEL FOR INFORMATION SECURITY

BMIS is primarily a three-dimensional model. It consists of four elements and six dynamic interconnections (DIs). The model is shown as a pyramid in **figure 2**, but it might be turned or distorted depending on the point of view of the observer. As a rule, all parts of BMIS interact with each other. Elements are linked to each other via the DIs. If any one part of the model is changed, other parts will change as well. In a comprehensive and well-managed information security universe, the model is seen to be in balance. If parts of the model are changed, or if security weaknesses persist, the balance of the model is distorted. The interdependencies amongst parts of BMIS are a result of the overall systemic approach.

Figure 2—Overview of the Business Model for Information Security



Source: Adapted from The University of Southern California, Marshall School of Business, Institute for Critical Information Infrastructure Protection, USA

The model addresses the three traditional elements considered in IT (People, Process and Technology) and adds a critical fourth element (Organisation). In terms of the information security programme, the flexibility and influence of elements and DIs vary. Some elements are comparatively inactive, but ever-present, such as the overall shape and design of the enterprise. It is there, but it should be seen as a boundary for the security management initiatives rather than an active and ongoing influence. Likewise, people are an important element, but not one that changes over time. Human nature will persist, and it is only through cultural change that behaviours will adapt to what the security programme intends to achieve.

The DIs are:

- Culture
- Governing
- Architecture
- Emergence
- Enabling and Support
- Human Factors

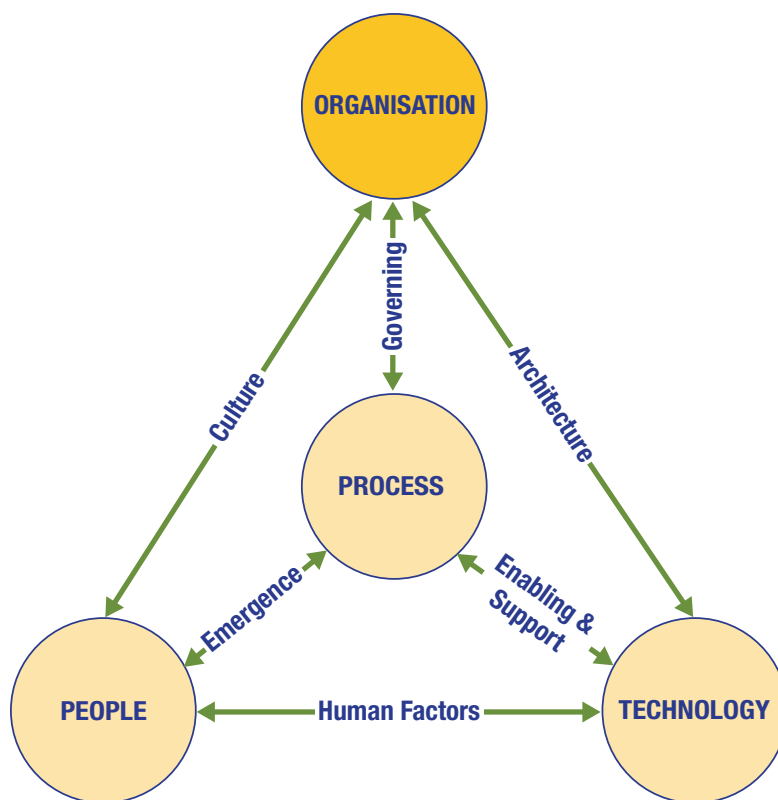
To obtain the maximum value from this model, it is important to understand that these DIs may be affected directly or indirectly by changes imposed on any of the other components within the model, not just the two elements at either end. The descriptions of the specific interconnections in this publication acknowledge this fact and provide examples of how changes to other model components can affect them.

## BMIS Elements

### Organisation

The Organisation element, shown in **figure 3**, is an important component of BMIS. It should be noted that the overall design of the enterprise is one part of this element, whereas the strategy is an overarching prerequisite that influences the Organisation element. Many traditional approaches to information security focus on the People, Process and Technology views of security, but do not examine the enterprise as a whole. They cover specific aspects of difficulties and problems observed, without including other aspects of the overall enterprise that may have contributed to these observations. These isolated approaches are often centered on technology or processes, but without an understanding of the surrounding forces that might neutralise the effort. BMIS provides a view of how the enterprise's design and strategy affect the people, processes and technologies, resulting in added risks, opportunities and areas of improvement. It further establishes a clear link between traditional security measures and the enterprise, including its influence in terms of design and strategy.

Figure 3—Organisation Element in BMIS



BMIS accepts the definition of Organisation as a network of people interacting, using processes to channel this interaction. Within the model's primary circle of Organisation, there are employees and other permanent associates. BMIS also links to external partners, third-party vendors, consultants, customers and other stakeholders. All of these internal and external relationships set the stage for operational effectiveness and, ultimately, the success and sustainability of the enterprise.

At the highest level, the perspective taken by senior management is intuitively systemic. The organisation is seen as a set of components that supports a set of common objectives. These are, in turn, formulated, revisited and communicated by the highest organisational level. At the lower levels in the organisational hierarchy, this holistic perspective is no longer a given. Divisions, departments or other silos often prevent managers and practitioners from seeing the big picture, and the systemic viewpoint is lost. As part of the BMIS Organisation element, the security programme should be seen as a value center because it enables the business to meet its objectives. Compliance, financial liability and legal issues are all important factors influencing the enterprise. However, they need to be seen in the context of organisational strategy and goals to make sense.

Through the organisation strategy that is a prerequisite to the BMIS element, security professionals can understand the core objectives of the enterprise and how the security programme should best support them. This can then be mapped to the security fundamentals of confidentiality, availability and integrity. Additionally, the strategy can act as a facilitator for conversations between senior management and security management. How the enterprise operates, sustains itself and innovates has long been a closely observed area that now needs to be applied to security.



## 2. BUSINESS MODEL FOR INFORMATION SECURITY

Organisational design theory is a thoroughly documented field. For quite some time, the structure of the organisation has been the focus, honing in on organisational charts, command structure, information flow, and accountability and responsibility for information. Likewise, academic professionals as well as practitioners have created a myriad of documents surrounding organisational strategy, examining the best possible methods to execute defined objectives. For the purpose of BMIS and its practical use, the design of the organisation simply supports the strategy. Once the overall strategy has been defined by senior management, organisational units, entities and other structures are adapted to the strategic objectives, which often involves restructuring. It is nevertheless imperative that any organisational design be secure, including the information it uses and the underlying IT subsystems.

---

**It is imperative that any organisational design be secure, including the information it uses and the underlying IT subsystems.**

---

Organisation structures differ depending on many circumstances, such as industry, size, geographic location and culture. However, regardless of the enterprise, there are commonalities. In practice, organisational structure is often put forward as an obstacle to achieving good information security. Some of the pros and cons of modern matrix organisations, as compared with the more hierarchical line or line and staff organisation structures, will always have an impact on the people managing information security. BMIS offers a business view on the intrinsic and cultural risks of any organisational design if these risks visibly impact security.

### The Formal Organisation

The formal organisation is the structure created by enterprise leadership and includes formal organisational charts, documented policies and directives provided to staff. It is complemented by the strategy set by senior management. Where the overall organisational strategy recognises information security as an important goal, the structure will reflect this in terms of design and people. In day-to-day life, the most effective changes in the perception of information security tend to happen when a senior individual at the board level assumes responsibility for security and reshapes the organisational culture. This usually helps reduce some of the ‘silo mentality’ that builds up if security is not seen to be a strategic priority. If, and where, organisational design and structure clearly support security as a priority goal, all subsidiary departments and units will become more efficient in working towards this goal. A well-designed security organisation can further improve the overall risk posture of the enterprise. The intuitively systemic view taken by senior managers will prevent unanticipated risks from arising in one area while attempting to mitigate risks in another—their strategic view allows them to recognise quickly the trade-off between various security-related risks.

The formal organisation is an important element to any enterprise. In terms of information security it is generally accepted that information security cannot be successful without the support and input of senior management.<sup>15</sup> In many organisations, hierarchical management styles are dominant, so if management does not prioritise security and communicate that priority to the enterprise’s people it will prove very difficult to get buy-in from business unit managers, gain adequate funding for the security programme and enforce policy. Likewise, if the enterprise is lacking structure, the same problems may be encountered but for different reasons.

### Example

In Company A, information security is part of the overall IT function. There is no chief information security officer (CISO) function, and the security manager reports to the chief information officer (CIO). The IT function sets direction by issuing policies and standards for information security, but it has no direct influence on the way these are implemented in the business units. Major decisions are made by committees, and then executed by the security manager.

In Company B, information security is centralised in a CISO role. Business units have formally nominated people responsible for security. Major decisions are usually made centrally, but they are often initiated from within the business. Security personnel frequently meet in regional groups, and sometimes on a global basis.

The two formal organisations are clearly different in their recognition of information security, and in their degree of central authority. Both may work, but there are other factors (such as Technology, Culture and Human Factors) that will influence the functioning of the security organisation. From a systems perspective, Company A is suffering from constant friction that arises from the somewhat autonomous actions of the businesses. Security managers often face changing practices and behaviours that are due to business pressures and day-to-day occurrences. However, these may conflict with central policies and guidance. The central functions in Company A have no direct link to the businesses, and any technical or cultural innovation is therefore difficult to consolidate. In Company B, the presence and participation of local and regional security managers create a self-reinforcing loop: the local tolerance for ambiguity and flexibility is put to the test (through regional and global meetings), and central units can provide feedback to the global organisation by identifying and encouraging best practices. In BMIS terms, the Organisation element will likely remain static in Company A, whereas the same element in Company B will be one of the instruments that help influence and improve information security.

<sup>15</sup> IT Policy Compliance Group, *Best Practices for Managing Information Security*, USA, 2010

**The security programme exists not only to protect business information, but also—and primarily—to support the business in reaching its objectives.**

The security programme exists not only to protect business information, but also—and primarily—to support the business in reaching its objectives. The formal organisation (within the element of Organisation) informs the security manager about what the business needs to accomplish in terms of information quality and the information assets to be protected. This knowledge is invaluable to the security managers because it shows them the direction that the security programme must take to achieve the most important objective: supporting the business by focusing on information assets rather than on general protective thinking. Accomplishing this objective enables others to recognise the business value that information security contributes.

## The Informal Organisation

While many organisations are very well defined and have ample policies and procedures in place for business operations, there also exists an informal organisation within the official organisation where things may operate outside of, or without, written policies. Organisational charts may document reporting relationships and delegated responsibility and accountability, but that is not always the way that information actually travels within the organisation. Furthermore, the informal organisation often determines how decisions are made, even behind the scenes and through influential individuals.

### Example

ABC Organisation hires a new security manager (Peter). ABC has little security in place, its budget is not massive and Peter reports to a very busy CIO who provides little direction but needs Peter to accomplish the seemingly insurmountable task of prioritising security so that incidents decrease while confidence and availability increase.

Peter would be wise to find out about the informal organisation. Who are the people with influence? Where is information handled? Where does information come from and go to, both inside and outside of the organisation? How can Peter bring the influencing individuals into the programme so that they understand how security will make their day-to-day lives easier? Can these influencers convince their peers, who are also influential and can support the programme?

It is critical that the information security programme recognise the informal organisation. With the direct connection to people via the Culture DI, there is a relationship between actions and behaviours, and organisational effectiveness. Behaviour patterns adopted within an organisation have a direct impact on security as well as on productivity and efficiency. In many cases, probably including ABC, they are the key factor to understanding how the organisation really operates.

The informal organisation ranges from a large subculture of individual employee actions to group subcultures that exist in individual business units. They are often linked to rewards and incentive systems. For example, sales teams are typically compensated based on individual and group sales rather than through a salary. Establishing an organisation goal and strengthening that goal through a reward system may create a situation where sales revenue is valued by sales personnel more than other important organisation goals. For example, controls that were implemented to prevent an exposure, such as data loss, may not be consistently followed, thus opening the organisation to legal or regulatory risks. In some sales organisations the use of mobile technologies may be used by sales people to continue to operate on the road although mobile technologies may not have been permitted or are restricted throughout the organisation.

Consideration may not be given to the use of security technologies such as encryption or secure communications or to risks related to how technology is used, such as concerns about social engineering. When there is a conflict between performance and conformance, controls may be avoided.

Sales teams are often awarded greater autonomy because of the importance of meeting monthly and quarterly revenue numbers. As a result, productivity can take precedence over policy. The same may not be true in other areas. For example, in the financial or accounting department, policies may be followed more strictly; in human resources, issues of confidentiality and protection of personal data come into play. These examples illustrate the distinct cultures that usually exist in different departments within the same enterprise. The informal organisation operates within these distinct subcultures as it does throughout the system as a whole.

## Organisational Impact on Security

How high-priority strategic objectives are formulated and then achieved has a significant impact on security. Productivity and profitability, financial stability and growth are balanced by compliance requirements, liability avoidance and limited appetite for risk. This balance between objectives and boundaries may differ even within business units or organisational departments, depending on the targets and their viability. Recognition of security as part of strategy varies greatly—in a customer-facing setting with real-time transactions, both the formal and informal organisation will easily see the necessity for strong and publicly visible security. In a compliance-based setting, the formal organisation may accept security as a given, whereas the informal organisation may show inertia and be reluctant to accept the associated cost. While the organisational strategy is therefore the driver for acceptance of security as a must-have, the organisational design and structure will impact the amount of maneuvering space that security management has—both formally and informally.



## 2. BUSINESS MODEL FOR INFORMATION SECURITY

It is imperative that the security manager understand, account for and address both the formal and informal organisations. A critical first step is bringing these areas actively into the security programme to create buy-in and to help shape the enterprise's security posture.

---

**It is imperative that the security manager understand, account for and address both the formal and informal organisations.**

---

The element of Organisation connects to the elements of People via Culture, Process via Governing and Technology via Architecture.<sup>16</sup> Changes made to any of these elements or DIs obviously lead to changes in the others. It is also critical to recognise that there will be implications to the entire system when changes are made.

### Example

In a large financial institution, the CIO receives an audit report on multiple security vulnerabilities relating to identity and access management (IAM). A new policy is developed that requires IAM to be more stringent than before. The CIO creates a task force to implement the changes and take charge of IAM. The identity management process is revised and communicated to all employees. At the same time, a new tool is introduced to globalise and centralise all IAM activities throughout the enterprise.

Subsequent events show an adverse effect. The number of access violations and shared identities rises sharply. Investigations by internal audit show that employees are reluctant to follow the new process as they feel it impedes their day-to-day business. Security managers can no longer control identities and access rights locally, and they have abdicated responsibility to the central unit now in charge of IAM. While the tool has been fully implemented, there are significant data quality issues that render it almost useless.

The initial change in this example relates to Organisation and the Governing DI (see the following paragraph). The overall system is changed by enforcing a new direction (globalisation and centralisation). As the Governing DI is activated, processes inevitably change. Likewise, the Architecture DI leads to the introduction of a new tool in the Technology element. Another effect on the overall model is the change in culture, as security managers no longer have local control over identities and access rights. This relates to the Culture DI.

The initial change in organisational design may have worked, had it not led to secondary effects in all other parts of the model: cumbersome new processes are met with passive resistance from people who feel unable or unwilling to adopt the cultural change. Their interpretation leads to Emergence (another DI): the process is followed, but not how it was originally intended. Similarly, the new tool cannot enable and support the new processes, simply because they are not followed as anticipated. While the architecture is there, it is dysfunctional.

In a linear mindset, the CIO's reaction to the audit report is understandable: findings are addressed by measures that are subsequently enforced until the number of IAM issues is brought down. In a systemic mindset, however, the CIO may have anticipated the primary effects on processes (slowdown, bureaucracy, sense of mistrust, etc.) as well as on culture (passive resistance) and architecture (introducing a tool that solves the wrong problem).

The Organisation element reaches into many business activities—including compliance, business continuity, resilience and sustainability—through its connections. It focuses on driving the business and steering the organisation towards meeting its objectives. It is a focal point for responsibility and accountability and a strong starting point for bringing security design into all business units in the enterprise. It also has the potential to influence substantially the culture of the enterprise. While risk management and convergence should be considered throughout the system, the primary area to address these topics is in the Organisation element. This reduces the danger of risk being managed in silos, inadvertently creating unanticipated risks to other areas of the business. With connections into the Process, People and Technology elements, the Organisation element will act as a driver to demonstrate the value of the security programme to the business and will have an enormous influence on the success of the information security programme.

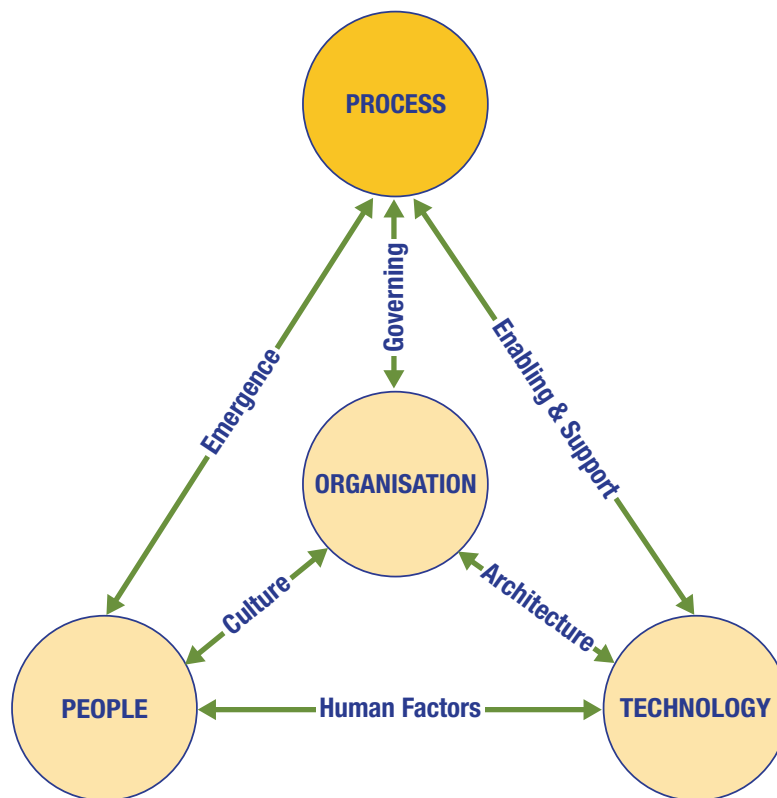
### Process

Process is the second element to be considered (**figure 4**). The Process element is unique and provides a vital link to all of the model's DIs. Processes are created to help organisations achieve their strategy. They are the structured activities that are created to achieve a particular outcome through individual or a series of consistently applied tasks. The Process element explains practices and procedures as people and organisations want them accomplished. Process is a fundamental element that symbolises the requirements for an enterprise to develop, promulgate, educate and enforce security practices and procedures in an ongoing fashion.

---

<sup>16</sup> The dynamic interconnections and related elements are explained in detail in subsequent sections of this document.

Figure 4—Process Element in BMIS



ISACA's Risk IT framework offers a clear, detailed description of an effective process as one that:

*...is a reliable and repetitive collection of activities and controls to perform a certain task. Processes take input from one or more sources (including other processes), manipulate the input, utilise resources according to the policies, and produce output (including output to other processes). Processes should have clear business reasons for existing, accountable owners, clear roles and responsibilities around the execution of each key activity, and the means to undertake and measure performance.*

## Attributes of Processes

Process attributes are:

- **Process maturity**—A process can utilise formal or informal mechanisms (large and small, simple and complex) to achieve its goal and serve its purpose. A process is generally considered mature when it is well defined, managed and measurable, and optimised. Informal processes can usually be performed only by individuals adept at the tasks and are either not documented or poorly documented. Amongst the few models that define process maturity are the COBIT maturity model for internal control and the Capability Maturity Model Integrations (CMMI).<sup>17</sup>
- **Link to DIs**—Process is a vital link to several of the DIs within BMIS, connecting directly to Governing, Emergence, and Enabling and Support. From the Governing perspective, a process is defined as an outcome of organisational strategy to achieve certain behaviour patterns while being enabled and supported by technology. From the Emergence perspective, a process needs flexibility to adjust and adapt to new and unexpected situations and take into account people's input as well as behaviour, based on experience and advice. Finally, from the Enabling and Support perspective, a process must be aligned with technology so the organisation can receive the full benefit from technical solutions on an ongoing basis. This works both ways: technology automates processes, but there may also be processes that empower technology, such as a help desk supporting a central software application.

## Systemic Approach to Processes

As a result, a set of effective security processes must span all aspects and areas of an enterprise. Process is a key element that will always touch on several other elements and DIs. It should be viewed holistically and not merely as the sum of its parts. A holistic approach defines the process as a complete functioning unit in which one part of the process enables the understanding and functioning of other parts of the process. There may not be a single information security process, and the BMIS Process element will usually consist of a large number of individual processes supporting aspects of security.

<sup>17</sup> For security purposes, the main implementation of the CMMI is in ISO 21827 Secure Systems Engineering—CMM.

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

### Example

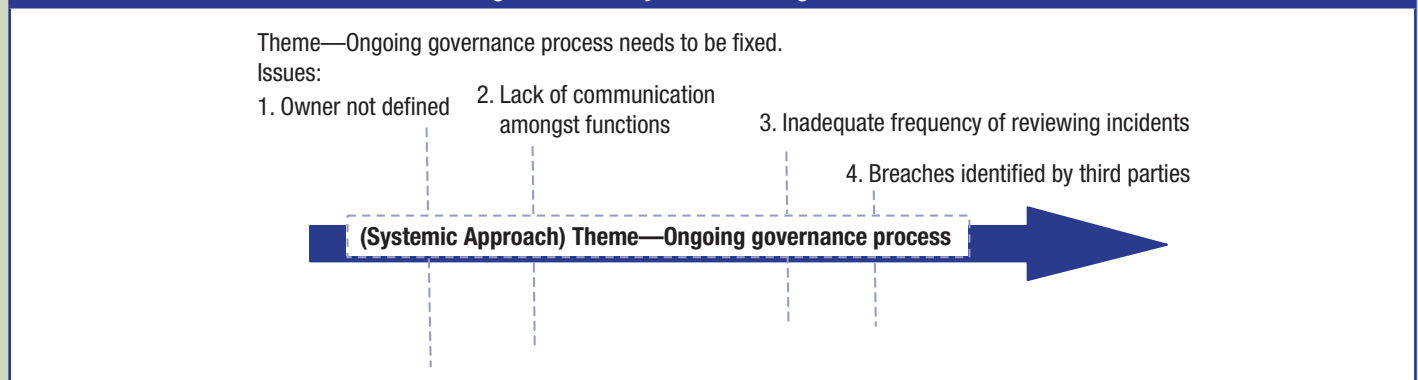
Process assessments are best performed by breaking each process into parts and analysing them either separately or holistically. Using the security incident management (SIM) process as an example, it is possible to identify the following common weaknesses/issues that are found in a typical SIM process:

- The owner is not defined and incidents are not reviewed often enough.
- Incidents are not properly classified and prioritised.
- Escalation paths are insufficiently defined and fail in practice.
- Incidents are not properly documented or managed, and there are no incident tracking tools in place.
- Incident follow-up is not performed and no 'lessons learned' procedure is in place.
- Resolution and emergency changes are not properly documented.

In a traditional (not systemic) approach, one would review each of these issues individually, often resulting in problem resolution efforts that attempt to address obvious symptoms without identifying the underlying cause. This, in turn, results in short-term relief but no long-term cure. For instance, in the issues listed above, it is apparent that the symptoms start with a failure to recognise the severity and priority of incidents, which often leads to weaknesses in documenting them. To the experienced reviewer, the list provides much more information 'between the lines': a lack of incident management skills may have been the root cause of being unable to classify and prioritise, whereas lack of senior management support (and budget) is likely to be behind the issues with documentation and tracking as well as lack of follow-up. Overall pressure on performance and day-to-day business priorities are the likely reasons for 'forgetting' to document the emergency changes that result from trying to resolve the incident.

In a systemic approach, on the other hand, one would identify all of the issues and then look for common themes that cut across them. In the SIM example, the theme can be identified as shown in **figure 5**.

**Figure 5—Security Incident Management Process**



In a systems thinking mode, the real reasons for failures in incident management quickly surface. The lack of ownership, and therefore the lack of responsibility, is the starting point for flaws in technique (classification, prioritisation). Where no one is really interested in incidents—and what denotes an incident in the first place—proper escalation is difficult to achieve. Likewise, an incident that has not been recognised for what it is will not be documented and tracked. The full picture clearly points in the direction of the organisational setup and the governance over incident management, whereas the individual observations (symptoms) look fairly technical at first sight.

Utilising a systems approach to information security processes can help information security managers address complex and dynamic environments. It can further generate a beneficial effect on collaboration within the enterprise, on adaptation to operational change, on navigation of strategic uncertainty and on tolerance of the impact of external factors.

Two other key concepts in systems thinking are feedback and delay. Feedback is the function of sharing observations, concerns and suggestions amongst persons or divisions of the enterprise for the purpose of improving both organisational and personal performance. From the security process perspective, feedback becomes a part of each security process in the model, allowing the specific process to 'learn', improve and adjust over time to respond to changing business environments. Feedback is necessary to adjust to the changing security threat landscape and to support improved security. In the previous example of incident management, the feedback from past incidents would be an invaluable tool to adjust gradually the governance framework, put a skilled person in place to fix the process, and address the flaws and shortcomings. With each successive incident, the person in charge would automatically receive information that is useful for the next steps.

# THE BUSINESS MODEL FOR INFORMATION SECURITY

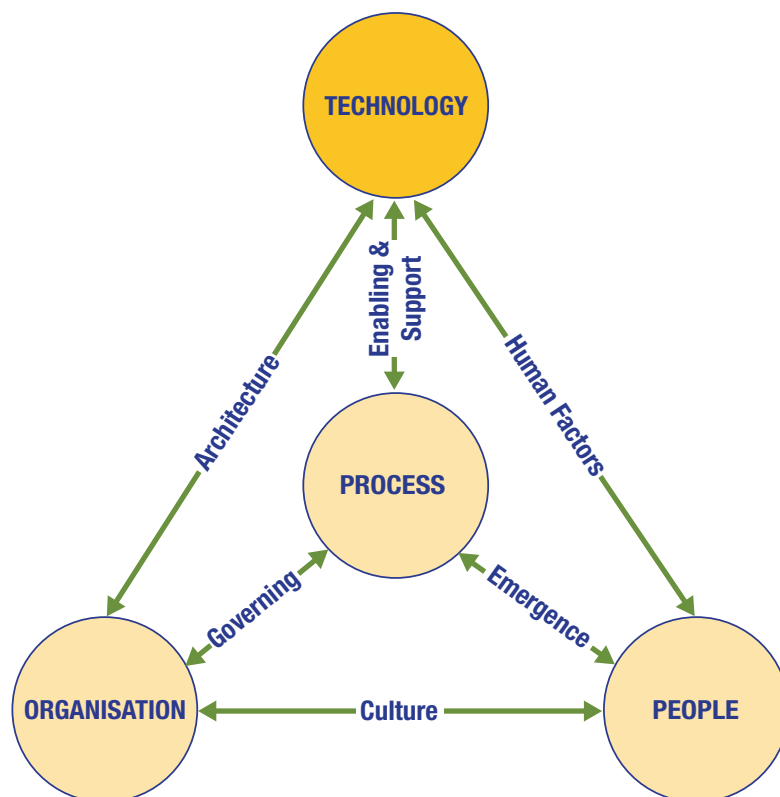
The concept of delay has implications to the model and to the associated security processes. Delay is defined as the period of time during which a process is operating when feedback is received and integrated into the process. The delay in performing the process or in implementing feedback creates risk in the model from the security perspective because it is a window of vulnerability for the enterprise. One example is the period between the time when a security patch for an operating system is released and the time when it can be installed on a system. Alternatively, how long does it take to protect all devices with the latest antivirus or antimalware software once released? And how does one protect the enterprise and others who have been updated from those who have not been updated? How does one address data leakage/protection from the time it is created and then deal with the impact of a delay in protecting it? In the incident management example, delays in recognising the symptoms and applying a systemic solution will leave the enterprise vulnerable to incidents that happen before the governance framework and the affected processes have been improved. Depending on the severity, these incidents may cause damage and have a significant impact on the business.

By using these concepts for processes, integrated with the BMIS model, organisations can leverage a systems approach to implement a more effective set of information security processes. To cover the whole of information security, a systems approach clearly spans more than one security process. As an example, the challenges in incident management should not be seen in isolation: they will obviously require senior security managers to look at links to disaster recovery and business continuity and possibly at the broader change management process and related procedures.

## Technology

Often the most familiar part of an information security programme, technology is a comparatively complex and highly specialised element within BMIS (**figure 6**). Technology gives security practitioners many of the tools used to accomplish the mission and strategy of the enterprise as a whole, including the generic security parameters of confidentiality, integrity and availability. However, technology is not all there is to information security, although there is a frequent misperception that investing in technology will resolve any and all security issues.

Figure 6—Technology Element in BMIS



## Scope of Technology

Technology can be defined as ‘the practical application of knowledge, especially in a particular area’ and ‘a capability given by the practical application of knowledge’.<sup>18</sup> The *Encyclopedia Britannica* defines technology as ‘the application of scientific knowledge to the practical aims of human life or, as it is sometimes phrased, to the change and manipulation of the human environment’.<sup>19</sup> These down-to-earth definitions illustrate the key meaning of the term within BMIS: technology includes every technical application of

<sup>18</sup> Merriam-Webster, USA, 2009

<sup>19</sup> USA, 2009

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

knowledge used in the organisation. In practice, the definition of technology is likely to be a narrow one since it serves the purpose of supporting and achieving organisational goals. In contrast, the thought that technology is just IT is too narrow. In the context of BMIS within an organisation, technology covers more than traditional IT.

At the lowest level, technology may refer to concrete objects (such as tools and implements) or to their workings. Alternatively, technology may be considered the amount of applied ‘scientific’ knowledge implemented within an enterprise and the degree to which the enterprise is dependent on it—the enterprise’s level of ‘technical sophistication’.

Technology, in the form of the increasing variety of options available, affects everyone’s daily life—from use of the camera and the car, to the television and video recorder, by way of the automatic bread maker. Thus, humans have tended towards a more concrete use of the term. Clearly, the possibility for mass confusion exists—and the puzzlement generated by these ‘at home’ examples is multiplied when the scene shifts to the enterprise. The confusion does not revolve entirely around IT; in most cases, IT is now able to offer safer solutions in the same way that the new generation of digital cameras minimises the risk of user error, the modern car contains a myriad of sensors linked to microchips that manage the vehicle’s performance, and the VCR can be programmed using simple, menu-driven input.

### Example

In a major international company, technology covers an unusually wide range of things. Basic infrastructures (such as water, electricity and roads) are seen as security-relevant in many regions where the enterprise has decided to take part or all of the responsibility for these infrastructures. This is often the case in more remote countries and geographic locations. At the other end of the technology range, core financial applications are also seen as security-relevant, for the obvious reasons. The different layers of infrastructure, IT and applications are managed through several technology departments that have defined links and interfaces (Organisation element). Several projects have been commissioned to integrate technology architecture and service-oriented architecture.

From a BMIS point of view, Technology is a pervasive element with a wide scope. The use of various layers enables distinction amongst processes that are supported, and the architecture of security-relevant technology is easily mapped. The safety and security considerations at all levels of technology are expressed by the Human Factors DI, which determines how technology is perceived, adopted and used. The systemic view allows security management to understand technology dependencies and effects on the overall system when changes are made:

- **Basic infrastructure (external)**—Electricity; heating, ventilating and air conditioning (HVAC); water; etc., may be provided externally, but they need to be seen as process enablers with a high level of criticality. In a systemic context, basic infrastructure influences all processes and people.
- **Middle layer IT (internal and external)**—Networks, hardware and platforms may be internal or outsourced, but they are dependent on the basic layer. They systemically influence both high-level technology solutions and processes.
- **High-level IT (internal and external)**—Applications, services, etc., depend on the middle layer of IT, including the security provisioning from that layer. They systemically influence both processes and strategy as well as people (direct users).
- **Pervasive IT**—Dispersed and decentralised applications, devices and processes are dependent on the high-level IT services provided by the enterprise. They systemically influence all other elements of the model and may reshape strategy and organisational design (paradigm changes in how people work).

In this example, the layers of technology link to different elements and DIs within BMIS. The complexity and wide scope of the Technology element need a detailed approach inside the element, but the systemic view ensures that dependencies and ‘ripple-through’ effects are identified and managed.

### Technology in BMIS

Thus, within BMIS, the Technology element refers to *every* implementation of technical skill and knowledge that could possibly have an impact on the general security of information. This could range from the personal pager and mobile phone to voice-over IP (VoIP); from the personal digital assistant (PDA) to the mainframe; from the solid building and physical lock on the door to biometric access management devices; from the PC camera to a fully integrated, color, freeze-frame video surveillance system; and from the fire alarm button to the most sophisticated fire detection and suppressant systems. As part of the systemic perspective, BMIS also addresses pervasive technologies that go beyond the boundaries of the enterprise itself: web-based applications and data storage, access via public networks, peer-to-peer infrastructures, darknets and other technologies that people use as services.

---

**Within BMIS, the Technology element refers to every implementation of technical skill and knowledge that could possibly have an impact on the general security of information.**

---



## Example

In a large international corporation, the cautious use of IT has led senior management to establish tight security controls and policies. These have been in operation for many years now, and copies of the IT security policy are distributed to every new employee who must sign a declaration of conformity. In a static security model, this is part of the 'people security' aspect that has been emphasised as important. In BMIS, the policy and control set are located in the Organisation element and the Governing DI.

The security policy was originally introduced in 2004, as stated in the footer of each page. It highlights the need for security and then goes on to describe in minute detail how diskettes should be destroyed, how employees should deal with modem dial-ins via public lines, and how downloads should be avoided when using narrow-band connections.

This shows how well-meant steps can be invalidated if the systemic context is not taken into account. In this case, the policy has not been updated and extended to cover 'smart' mobile devices (it barely mentions laptops), wide local area networks (WLANs), the universal mobile telecommunications system (UMTS), peer-to-peer darknets such as FON, or service-based devices that serve only to access the web where data are stored and applications reside (for example, the Google phone). While technology is being addressed, this is done in a linear way rather than in a systemic way.

New technology is generally restricted in this corporate environment. The first answer senior management and IT will give to a user is a strict 'no'. Only after several innovation cycles will the no-longer-new technology be internalised and authorised for general use. Users in this large international corporation are therefore lagging behind in using fast technology and typical enablers of their day-to-day business.

Within BMIS, it is immediately apparent that there is a mismatch between the intent of the policy and the technology on the ground, as the policy has become obsolete. The way to resolve this is obviously in the Architecture DI, which must provide the link between existing (or planned) technology and the organisational assumptions relating to security controls. Walking through BMIS step by step, the overall organisational strategy appears to be unfriendly to technology, and there is a disconnect between the corporate view of the world and the real world. The Process element, as governed by policies and controls, is therefore likely to be lagging behind the current state of IT usage and security. Furthermore, people/employees will have grown used to more modern ways of working, most likely through their private use of IT at home. In systemic terms, this creates tension between the organisational culture and people's habits and behaviours. This may lead to subtle changes in processes that come about through the Emergence DI. In practice, a typical example is when employees start bringing their private laptops into work to avoid having to use the corporate IT structure.

## Example

In a regional firm in Europe with approximately 1,000 employees, technology is part of the organisational fabric. The core business is manufacturing high-tech equipment that is exported to many countries globally. IT is generally seen as an enabler for day-to-day business, and security is very high on the agenda due to various patents, other intellectual property rights and a couple of interesting new prototypes in the pipeline.

While the company has an information security policy, this policy is entirely behavioural and says little about technical controls. In essence, it just states that every employee should handle data and information just as they handle their personal e-banking data, regardless of the hardware or software used. The policy further states that, in principle, nothing is restricted—but the risk should be assessed and evaluated by employees as they would do with their own credit card data.

New and disruptive technologies are quickly adopted into the organisation. When a 'new thing' is available in the marketplace, there are always several people willing to test it, report the results back to IT and subsequently work with IT to make it secure. Users drive the process of adopting, adapting and accepting new technology, and other users benefit from the pilot schemes. In this way, the company has internalised smartphones and even the first wearable computing devices.

In BMIS terms, the Organisation element is much less important in this case than in the previous example. Technology is driven by the People element and the Human Factors DI, as users are encouraged to adopt new technology on a test basis. The organisational culture is therefore more people-centric and less focused on central governing and control. In following processes, users actively seek out technology and strengthen the Enabling and Support DI. From a systemic perspective, this BMIS view is much more dynamic than the previous example. The company in this example relies much more on the Culture and the Human Factors DIs than on central governing and architecture considerations.

Neither of these examples provides a definitive answer to what is right or wrong. However, both examples show that BMIS as a systemic tool clearly highlights the role of technology as an element.

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

It is fair to say that the Technology element contains exceptional capability for addressing security weaknesses. Many information security concerns can be satisfied by the implementation of technology-based controls, including those concerns related to human error or deliberate attack and the impact of natural or man-made disruptive incidents.

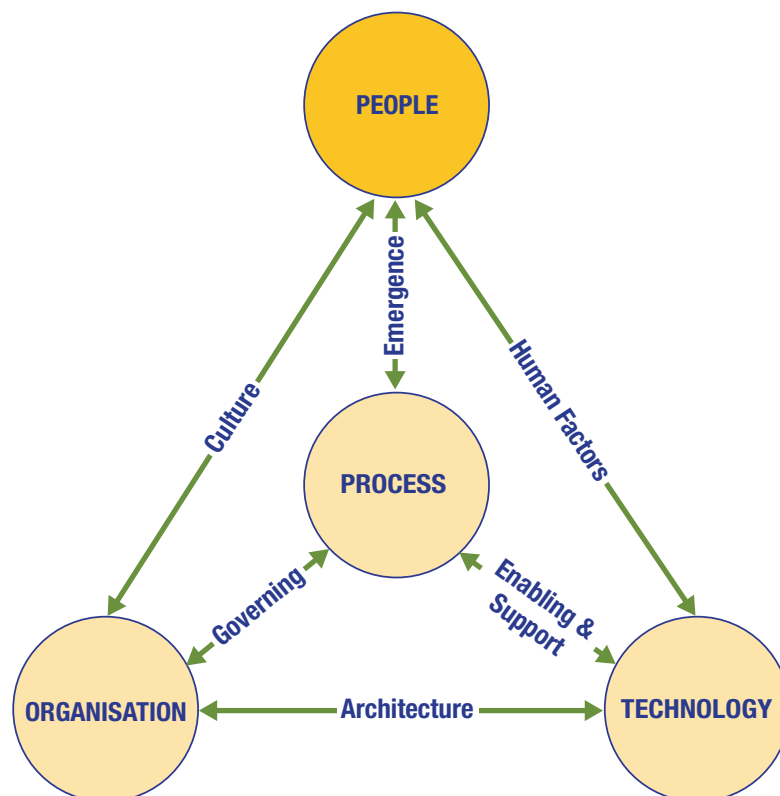
Once a tool used mainly for perimeter protection, technology has advanced through the years to provide protection not only for the perimeter, but also for areas such as data loss prevention, encryption methodologies, event correlation, access control and information management. While there are many options for the tools, enterprise risk and business process risk are the driving forces behind the security programme. Technology selection should therefore always address the utility, efficiency and productivity of the overall enterprise. Once the technology is selected and implemented, training must be given to those who need to use the tools and monitoring will be needed to verify that the technology is functioning appropriately. There have been many recent and well-publicised breaches from enterprises with loads of technology in place to prevent security events. While technology is an important piece of the puzzle, if it is implemented and ignored, it can give the enterprise a false sense of being secure.

### People

BMIS's People element (**figure 7**) represents the human resources in an organisation—the employees, contractors, vendors and service providers. The primary people within BMIS are those who are employed or otherwise associated with the organisation. However, in outsourcing situations, multiple vendor relationships or managed-services technology solutions, there is a second circle of people who indirectly work within or for the organisation. This wider circle of people needs to be considered, but their impact on security may not reside in the People element. For instance, a provider of help desk services may be seen as a process within that element, and any people-based systemic effects would be through Emergence. In practice, the end result of a systemic change regarding people is often the same—regardless of whether the people are internal or seconded externals.

'People' are not just units of one and they cannot be studied in a standalone manner. To understand how information security affects, and is affected by, people, a systemic approach is required, studying people's interaction with the rest of the elements of the model through the DIs.

Figure 7—People Element in BMIS



People within an organisation have their own beliefs, values and behaviours arising from their personalities and experiences. The corporate framework affects, and is affected by, these attributes since it defines its own beliefs, values and behaviours and the degree to which people are expected to comply. This is reflected by the Culture DI. For example, the way people act within an organisation—and relative to information security—depends on the corporate human resources (HR) strategy as defined in the Organisation element and implemented within processes, as part of governing the organisation. If the corporate HR strategy relates

employee performance in complying with corporate policies (including information security) to employee evaluation results, then compliance with the corporate culture is being supported. In another example, the enterprise that has well-developed policies for dealing with employees during hiring and employment and after contract termination demonstrates a strong process for managing people and expectations relative to information security. Of course, this process is implemented by people (the HR department, line management, the security department) and human nature dictates that, when implementing processes, people often introduce a level of uncertainty, which is reflected by the Emergence DI.

It is evident that people influence information security through their interaction with the corporate environment, reflected in its corporate strategies and processes or in other people. A study of other elements and DIs, such as Technology, Human Factors, Enabling and Support, and Architecture, will enable a better understanding of this interaction. For example, people may have been hired because they demonstrated certain abilities to use technology. But if information security is implemented within the corporate technological infrastructure in a manner that is contrary to the prevailing corporate culture, those same people may have difficulty in complying with the security policy, regardless of their technical skills. If the system designer does not have the requisite level of skills and security knowledge, it is likely that both the user-friendliness and the acceptance of the identity system will be low.

As an example, if an enterprise attempts to reduce theft by utilising technology such as a badge reader or a code for physical access control, it would behoove the enterprise to communicate the change to employees in advance. If the technology is then deployed in a well-controlled manner that includes training, communication of the reasons for the new control and explanation of the policies associated with it, management may forestall employee aggravation (and its possible manifestation in overriding controls by propping open doors, letting people in or even physically damaging the device).

Likewise, if an enterprise requires password changes too frequently, or if passwords are overly complex, the outcome will be bureaucratic overhead on the process of password management. Thinking systemically, the gain in security (against passwords being guessed or brute-forced) turns into a loss in security because human factors come into play. The overall system risk—from the perspective of senior management—has increased rather than decreased if people are unable to cope with complex password management and subsequently share passwords or write them down. The decisive element in this example is People, as their perception of ‘having a password’ and their reaction to frustration will trigger the Emergence DI and consequently compromise the process.

---

**In BMIS, the central element that decides on acceptance of controls is People.**

---

These situations occur because the security controls implemented, although well-meant, were confusing, difficult to use or aggravating. It is possible that after implementation of such controls, the enterprise is more at risk than before because the implementation has generated a false sense of security. In BMIS, the central component that decides on acceptance of controls is People. While they are expected to adhere to certain rules and restrictions, individual human nature may lead to a variety of different outcomes. The Human Factors DI triggered by an acceptance problem

can easily invalidate the technology (which might be solid and workable when seen in isolation). The Culture DI, on the other hand, determines the unwritten rules in addition to the written rules—people will most likely follow what they see as the prevailing corporate culture or peer group culture. The Emergence DI results from individual or group behaviour patterns and directly influences the password management process.

If employees avoid the process or do not follow the policies, there may be additional risks, as well: When security is seen as cumbersome or too complex, people tend to make their own unwritten rules because they are unable or unwilling to accept the written rules. Conversely, if employees are facing an increasing number of controls, procedures and other norms, they may follow them to the letter, but without realising the rationale. Thus over-control can gradually replace cautious thinking and active attention to security.

Anyone accessing information and performing a process (or part of a process) on the information should be made aware of the quality requirements (how value is added to information by the applied process) and related security controls (to ensure that this level of quality is reached). This is addressed by the Process element through the Emergence DI, by which people may participate in elaborating the most appropriate and safe process. This will be much more effective and efficient if the organisation provides clear direction and objectives and the appropriate culture motivates everyone, not only to perform the security tasks consciously but also to enhance their effectiveness and efficiency. Supporting the controls with tools (technology) will predispose people to use them adequately, provided the controls and tools are appropriately explained and they do not make it more difficult to accomplish day-to-day work.



## 2. BUSINESS MODEL FOR INFORMATION SECURITY

### BMIS Dynamic Interconnections

The elements of BMIS, as described previously, do not exist in isolation. In traditional security approaches, the dependencies amongst elements are often overlooked. This leads to linear thinking and escalating steps and measures in one element, but without necessarily achieving real security improvements. It is often obvious that, in practice, changes to one element influence all other elements. The way in which BMIS expresses these dependencies is through DIs.

Any DI between two elements is flexible and also represents the potential tension between the elements. As an example, the Organisation and People elements are closely linked, but many of the difficulties known in day-to-day business stem from the fact that the given organisation structure does not match people's expectations. Likewise, the Enabling and Support DI between Process and Technology obviously exists, but it may be strained at times when new technology does not entirely fit the existing processes. Tensions in DIs generally distort the model and, in the course of time, lead to changes that lessen the tension between elements.

The interconnections also signal that BMIS is not static. They represent the dynamic parts of the model in which actions occur and where changes, in turn, influence the elements. Human nature tends to remain consistent, regardless of whether people are within an organisation or outside of it. Similarly, the adoption of changes in organisational strategy happens in a series of steps, and sometimes slowly. However, the Culture DI between Organisation and People is subject to frequent change, and in systemic thinking, culture is more than the sum of its parts.

The DIs in BMIS also interact with each other in a systemic sense. In some situations, the behaviour of the overall system creates feedback or feedforward loops. These loops dynamically change the system and gradually move it to a new state. Where tensions exist that distort the model, changes will arise first in one DI and then in the corresponding elements. This, in turn, may influence other DIs and elements, leading to a loop that is self-reinforcing and moves the model as a whole.

---

**The interconnections also signal that BMIS is not static. They represent the dynamic parts of the model in which actions occur and where changes, in turn, influence the elements.**

---

### Governing

According to ISACA, 'governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly'.<sup>20</sup> Enterprise governance and governance of IT set the global boundaries for what is feasible within information security. As such, governance lies outside of, and touches, every aspect of the BMIS model. Enterprise governance, amongst other things, influences the form that an organisation takes as well as how the People, Process and Technology elements come together to support the mission and strategy of the organisation. The Governing DI therefore translates existing governance concepts and measures (at the level of the Organisation element), encouraging organisations to meet their missions and goals and establish boundaries and process-level controls.

Acting as the connection between the elements of Organisation and Process, the Governing DI (**figure 8**) represents the action of putting governance into practice within BMIS. This means managing the process while implementing the sense of direction set by senior management. While the two elements represent what needs to be done and how to do it, this DI acts as a catalyst to actually getting it done. Governing is achieved through the interconnection with the Process element. The rules and regulations—i.e., standards and guidelines—are reflected in the Process element through defined or *ad hoc* procedures and practices.

The feedback loop that actively modifies the Governing DI results from the other DIs of Culture and Architecture, acting on design and strategy. For example, to the extent that the Technology element is inadequate to serve the organisation's security needs, the Architecture DI will create 'tension', distorting the model and resulting in the need for changes to the design that will, in turn, modify the strategy that changes the Governing DI. Changes in the Governing DI will modify procedures and practices in the Process element.

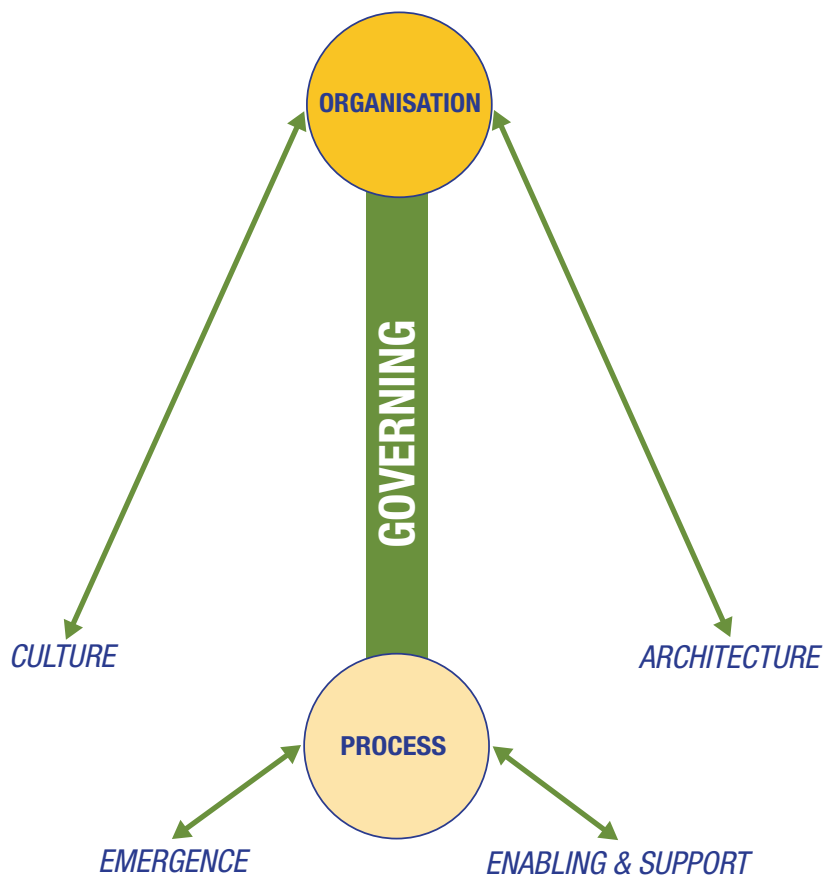
### Objectives

Processes must serve the objectives of the organisation at an acceptable level of predictability, i.e., risk. The act of governing must set the focus for what needs to be achieved in the various organisational processes (Process element) and concurrently set the limits on activities that mitigate risks sufficiently. Governing must also address issues of organisational preservation, or sustainability, and do so without unnecessarily limiting the ability of the organisation to prosper and thrive.

---

<sup>20</sup> ISACA, *Board Briefing on IT Governance*, 2<sup>nd</sup> Edition, USA, 2003

Figure 8—Governing DI



## Approaches

Governing encompasses all tactical activities required to achieve the organisation's strategy within the context of organisational design. Any governing activity that does not meet these criteria will be counterproductive and create excessive 'tensions' that must be resolved through changes in design and strategy or in the Governing DI. Excessive governing beyond what is needed to achieve business objectives and limit risks to acceptable levels becomes a constricting bureaucracy, reducing organisational adaptability and resilience in dealing with emergent situations.

The primary tools for governing are standards and guiding actions that demonstrably meet policy intent. Standards that are not providing the right set of boundaries and guidance will result in an unacceptable risk exposure for the organisation. Standards that are too restrictive needlessly limit procedural options and negatively impact organisational resilience, adaptability and effectiveness. Likewise, other guiding actions—representing governing in the active sense of the word—should be linked to the organisational strategy and the resulting objectives. Every action taken in terms of governing must have a clear justification and rationale, particularly those that influence and shape security processes. Governance—and, therefore, the Governing DI—includes, but is not limited to:

- Policies
- Standards, guidelines and other normative documentation
- Accountability rules
- Resource allocation and prioritisation
- Metrics (for all of the above)
- Compliance (as an overarching theme)

Communication is vital within the Governing DI. Governing must filter down in the organisation through all levels of management via appropriate channels. To achieve optimal effectiveness, it must be intrinsic to the culture as well as practices and processes of the organisation. Security requirements—often merely good practices—must be addressed in all job descriptions and those responsibilities and accountabilities reinforced on an ongoing basis through training and awareness campaigns.

Many of the issues that information security addresses result simply from poor or inadequate design or process or the failure of the culture to value conscientiousness sufficiently—often an outcome of focusing solely on performance. If unchecked, processes may change over time and develop their own ends and means, mainly to achieve ill-understood objectives or to accommodate increasing

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

pressure. Governing will require realigning all processes with both the objectives of business and the amount of risk associated with doing business. It is management's responsibility to subsequently enact the processes and to be mindful of risks and overall objectives.

Effective risk management demands strategic leadership, and the responsibility and accountability for security must be placed directly in the hands of the board and senior management executives. In many enterprises, security is seen as a low-level technical (or even IT) issue rather than a strategic requirement. The result has been evident in the continuing headlines reporting ever more spectacular security compromises. Once again, BMIS inserts the Governing DI as a means of dealing with the tensions that may exist between organisational strategy and security processes. For instance, processes subject to exaggerated cost-cutting may result from an ambitious cost reduction strategy that has been set by senior management. In this instance, governing is the act of defining 'must-reach' security levels, acceptable cost items and 'must-have' investments in security.

All governing activities must be explicit and are a required part of organisational design and strategy with defined links amongst design, strategy and process.

Frameworks/standards that support the Governing DI include:

- COBIT<sup>21</sup>
- Val IT
- COBIT Security Baseline
- Risk IT
- OECD Principles of Corporate Governance
- ISO 27000 series—Information Security Management Systems
- COSO Enterprise Risk Management Framework
- NIST SP 800-53—Recommended Security Controls for Federal Information Systems, for more IT-related issues

### **Culture**

While technology and policy remain important ingredients in securing enterprise information, it has become obvious that they are not sufficient on their own. Culture (**figure 9**) is one of the DIs that separates BMIS from other security models. By addressing culture and its impact on behaviour BMIS provides a more complete picture of the enterprise. The impact of culture on people is a key issue in information security since people are able to contribute to the security of information or, conversely, to compromise it.

The Culture DI affects, and is affected by, the elements of Organisation and People—logical relationships because the internal culture of the enterprise can be related to the cultural influences on the individual. The synergy between human resources and the organisation is the foundation for the corporate culture.

### **What Is Culture?**

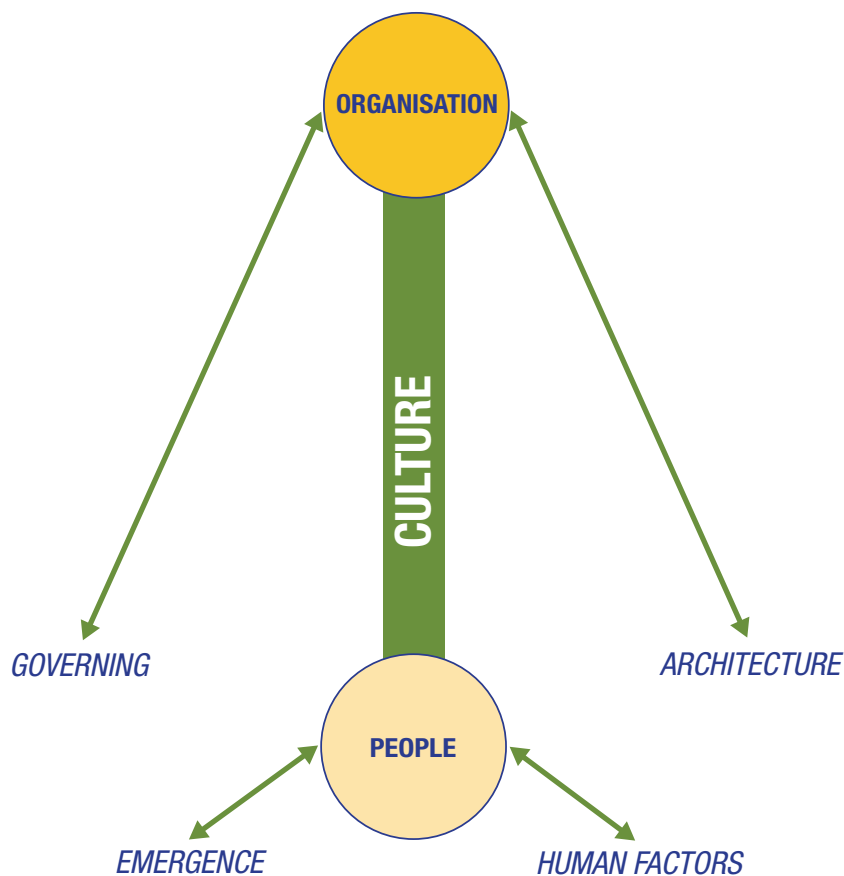
Organisational culture is a broadly documented topic for which many definitions have been published. The definition that BMIS utilises is: 'Culture is a pattern of behaviors, beliefs, assumptions, attitudes and ways of doing things'.<sup>22</sup> The word pattern is key in this definition. Cultures are made up of individuals, but do not necessarily represent individual behaviours. It is culture that influences individual and group behaviours. In using BMIS, there are two layers of culture to be considered. The organisational culture is formed over time by strategy, organisational design and people's behaviours at work. The second layer is found in people's individual culture, which may be diverse and heterogeneous. Both layers must be taken into account when viewing Culture as a DI that influences security.

People are the key to culture, and culture, in turn, creates a set of perceptions in people. In addition to internal organisational factors such as compensation, praise, promotion prospects and other managerial policies, perceptions are influenced by factors external to the enterprise, such as religion, ethnicity, socio-economic background, geographic location and personal experiences. These external factors—which on the surface may not appear to have much impact on day-to-day operations—manifest themselves in behaviours brought to the workplace and are often much more important than expected since they form foundations for workplace behaviours and norms.

<sup>21</sup> COBIT has been mapped against many of these standards to facilitate integration: [www.isaca.org/cobitmapping](http://www.isaca.org/cobitmapping).

<sup>22</sup> Kiely, L.; T.V. Benzel; 'Systemic Security Management', *Security & Privacy, IEEE*, vol. 4, no. 6, 2006, p. 74-77

Figure 9—Culture DI



**To improve the information security programme, managers need to examine and understand the culture that exists within the enterprise, and then they must extend the culture's strengths and recognise or improve its weaknesses to create a culture that is truly intentional in its approach to security.**

To improve the information security programme, managers need to examine and understand the culture that exists within the enterprise, and then they must extend the culture's strengths and recognise or improve its weaknesses to create a culture that is truly intentional in its approach to security. It is no small task to enhance or change a culture that is set and has operated in a particular way for any length of time; however, it is a critical step in improving the overall risk posture of any enterprise. Subsequent steps in creating a security culture go beyond the mere understanding of existing culture. However, realising what already exists is an important first step. Changing or enhancing a general organisational culture is an endeavor that is, by definition, limited since people in themselves are unlikely to change drastically. Therefore, it is important to recognise the limitations of changing the second (people) layer of culture. It is possible, however, to change the first layer, which is the organisational understanding of expected behaviour and the understanding of security, and this should be the aim of steps taken in forming the security culture.

Cultures are as different in organisations as the underlying characteristics that form them. Corporate culture is often thought of as a product created by senior management through rules. While it is correct that leadership has a strong influence over the culture of the enterprise, culture is actually created by the patterns of people's behaviours and attitudes, which are influenced by their perceptions and beliefs and sometimes even by habit and tradition.

Systemic security management (SSM) research identifies six aspects of culture that are of particular importance to information security issues, and ISACA's Risk IT framework adds a seventh:

- Rules and norms
- Tolerance for ambiguity
- Power distance
- The politeness factor
- Context
- Collectivist vs. individualist<sup>23</sup>
- Risk-taking vs. risk-averse<sup>24</sup>

<sup>23</sup> Kiely and Benzell, op. cit.

<sup>24</sup> ISACA, *The Risk IT Framework*, USA, 2009, p. 22. Risk culture forms an important part of security thinking.

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

While some of these aspects may seem familiar, they also highlight less common concepts such as the politeness factor, in which people are afraid to correct their superiors or peers so as not to embarrass them; the tolerance for ambiguity, which examines how well the enterprise deals with the unknown and with change; and the collectivist vs. individualist mindset, which focuses on how to get employees away from 'me' to focus on 'we'.

In addition to the aspects mentioned, enterprises must consider the effect of factors such as geographic location, ethnicity and religion. For example, many countries, whether through the influences of religion or tradition, have a culture of trust. The default values of management are to trust the integrity of employees, suppliers and customers. Some consider trust the very basis for business since trust is the willingness of one party to be vulnerable to the actions of another party, based on the expectation that the other will perform a particular action important to the first party. At one time, when the world of finance, commerce and industry was more stable, these traits might have been a reasonable assumption. However, in an environment of globalisation this is an area to which the information security manager must pay close attention. 'Trust no one' is one extreme that should be avoided as should the (frequently seen) other end of the spectrum: 'We all trust each other around here'.

Because all enterprise cultures (the first layer of culture seen from a security perspective) have their own flavor, it is important for the information security manager to understand that what is best for the organisation is important for security culture: if people are loyal to the enterprise, they are more likely to handle information in a secure manner. Well-established and well-communicated strategies and goals can help organisations grow from the 'me' perspective to the 'we' perspective. Ideally, this means that regardless of formal security policies and procedures, people are likely to develop a mindful perspective on protecting information, just as they would when protecting their own homes. However, this entails management and staff sharing a common understanding; only where enterprise culture is not just understood, but shared, will the overall result be acceptable.

### Example

In an Asian company that provides outsourced services to many European and US enterprises, security appears to have been well communicated, documented and 'lived'. An unplanned inspection reveals that on the day before the announced audit, most of the security rules are openly breached, and there is a significant difference between the situation as observed and as seen in prior audits. On interviewing management, the auditor learns that 'the visit had not been announced and was planned for the following day'.

From a BMIS perspective, this example shows two things. First, culture as defined and communicated is something that local staff and management have understood, but not internalised. It appears that customers' expectations are met to the best of people's ability, but only when an audit takes place or some other mechanism of surveillance is in place. In all other instances, the security expectations voiced by the customer are, at best, seen as strange and politely ignored. Second, people's individual culture, and perhaps the local culture as a whole, are obviously entirely different from the prevailing culture in the customers' home countries. This creates considerable tension in the model's Culture DI.

To resolve these cultural discrepancies, BMIS would indicate actions in the Culture DI, for instance, through inserting expatriate individuals in security management or seconding local security managers to the home countries of the enterprises outsourcing to Asia. Regardless of the security model applied, it is likely that this process of slow cultural adaptation may take a long time.

# THE BUSINESS MODEL FOR INFORMATION SECURITY

## Example

In a manufacturing company in Germany, security management observes frequent occurrences of virus infections, malware and unauthorised applications being downloaded to the corporate network. For a long time, senior management has maintained a strict security policy, coupled with a culture of detailed guidance and wide-ranging enforcement including disciplinary action and dismissal. An audit reveals that, with the increasing use of the web and Web 2.0 applications, employees have inadvertently started to take higher risks. As a result, the number of security incidents has increased significantly. There is an obvious tension in the Culture DI.

An analysis from the BMIS perspective shows that there is an 'old' security culture which is not uncommon in manufacturing firms: strict security is part of the business model and all trade secrets are well protected. This protective culture is obviously well understood and accepted by employees since the problem seems to be centered on IT and not the other business processes. The 'new' security culture, on the other hand, has not yet formed and employees appear to be using the web in an unguarded—and unguided—way. They have been trained to work according to a strict set of rules, and they are less well equipped to exercise caution when there are no rules. This is confirmed by employees stating that they 'did not do it on purpose'.

In this example, the problem of information security breaches is later resolved by bringing in an external consultant who trains employees 'on the job'. An encapsulated network is set up that simulates the typical use of the web and Web 2.0 applications. Employees are given practical demonstrations of how to deploy a virus, how to insert malware, etc. After a few sessions, which prove to be enormous fun to the employees being trained, the overall number of security incidents decreases sharply.

While enterprise cultures are unique, they do fall into certain categories. Each of these categories has characteristics that describe the way the people associated with the enterprise interact, the prioritisation of creativity and innovation in the way the enterprise operates, the enterprise's ability to deal with ambiguity, and its tolerance and flexibility in regard to change. These characteristics form the basis of the organisation's culture and are often part of the enterprise's core values.

## Example

In a hierarchical or militaristic culture, the dominant idea is one of command and control. Strict adherence to orders is a given, and decisions are made in a strictly hierarchical manner and in accordance with rank. Executive management pushes down its beliefs and preferences and runs the business in accordance with those beliefs. These types of organisations have defined structures and may leave little room for employee input or innovation. The perceived advantage of these rigid cultures is the predictable functioning of large groups of people at a defined level. Military forces, particularly in peacetime, are often seen as bureaucratic, slow and inefficient. However, their primary purpose is efficient and completely predictable functioning in wartime so there are no surprises and so total reliability is ensured.

Other cultures are more egalitarian in nature, viewing all staff as equal and considering rules as less important than productivity. In these cases there may be a lack of structure and people are often left to their own devices as to how to deliver. Security concerns are often evident because people choose to circumvent existing controls or procedures to produce output quickly. Security may not be enforced consistently, so behaviours become norms and security is generally avoided.

Problems exist in both types of atmospheres. For example, within a hierarchical culture the power distance is high. In this situation executive management tends to be authoritative and demands employee adherence to strict rules. Employees may follow security policies out of fear of consequences. This culture does not help employees appreciate or understand security. The perception may emerge that security makes things more difficult or acts as a roadblock to getting the job done.

Likewise, an enterprise in which management is *laissez-faire* and focused primarily on productivity has a lower power distance, i.e., it may lack structure and well-defined policies or it may have policies that are not enforced. The perception is that security is optional or is secondary to getting the job done.

As can be seen, neither type of environment makes for a 'better' security culture. In fact, both give rise to potentially serious issues. In the first example (a culture with a high power distance), employees may be so tied to the policy out of fear of noncompliance that they may not be able to recognise an emergent issue or undocumented threat as a possible risk to enterprise information assets. As long as they have followed the rules, they feel safe without having to think 'outside the box'. Likewise, in a culture with a low power distance, people may ignore procedures or avoid controls to get their jobs done quicker, creating potential risks. When confronted with a security incident, people are likely to point out that 'security is not what we are here for; we have a job to do'. A balance between these two types of environments would most likely create a better security culture. However, most enterprises do not have the perfect mix of flexibility and structure, so change is needed.



## 2. BUSINESS MODEL FOR INFORMATION SECURITY

### Creating the Security Culture

The organisational culture affects the entire enterprise system. Being prepared to deal with change is essential. Some types of cultures are more open to dealing with change than others. As culture is often the most important factor accounting for success or failure of an organisation,<sup>25</sup> it is of critical importance that security professionals strive to create a culture that not only realises the importance of information security, but also embeds information security into its day-to-day operations. By implementing expectations and desires in a security culture, organisations may be able to use the culture to actually improve enterprise security.

---

**By implementing expectations and desires in a security culture, organisations may be able to use the culture to actually improve enterprise security.**

---

Creating a security-conscious culture is not an easy or quick task, but rather a long-term objective that should be considered by everyone within the enterprise. People are a consistent component to information protection. All of the people who make up an enterprise—from the board of directors and executives to staff at all levels—and companies with which the enterprise has third-party relationships have the ability to improve information security or to weaken it. If people behave with security in mind and incorporate information security practices into their daily activities, there is a much better chance of keeping enterprise information assets protected.

People are not generally malicious, but they are sometimes unaware of security policies, unsure of how to put the policies into practice or unwilling to follow security protocols. Security awareness and education are helpful and necessary, but not adequate on their own. Real change needs to occur in the front line of the organisation where culture is established. Regardless of an enterprise's current culture, it is important to understand that culture can be changed, and this change—from reactivity to proactivity, and then from proactivity to intentional and enshrined security—must be considered a core objective of the security programme.

By influencing the culture of an enterprise to become more conducive to information security, the strengths of BMIS can be harnessed to improve the overall security posture of the enterprise. Cultural changes must be viewed on a systemwide basis. In other words, improving the culture does not happen simply by instituting a robust awareness and training programme, getting buy-in from executives or changing procedures to incorporate secure practices. All of these measures, and more, are needed to effectively change a culture over time.

Some first steps to enhancing the culture to be more favorable to security can include the following:

- Work to establish a strong information security programme that includes buy-in from enterprise leadership and functional business unit leaders. Find influential leaders throughout the enterprise to help deliver key messages.
- Establish, communicate and enforce clear security policies.
- Encourage collaboration amongst business units, thus reducing siloed management.
- Work to have security responsibilities included in job descriptions and annual performance reviews for everyone.
- Gain concurrence on clear goals and objectives.
- Provide the knowledge, tools and skills that people need to effectively handle information assets.
- Develop consistent processes for information handling and sharing.
- Develop scenario training to influence change in beliefs and attitudes.
- Work to change negative perceptions of security.
- Communicate, communicate, communicate.

As shown previously, changing a culture requires many activities that are constant and consistent and involve people at all levels of the enterprise. Consistency will help ensure that the activities begin to evoke desirable behaviour that transitions into unwritten (and later written) norms. Small intentional changes can have cascading effects across the enterprise. Increasing collaboration amongst groups can increase trust and bring people together with a common goal. Once people begin to work together, they can begin to share experiences, which will help improve relationships and attitudes and demonstrate commonalities.

The security culture matures as the patterns of behaviour adjust so that security becomes engrained into daily activities. As training and awareness expand, awareness is enhanced and individual business units or groups begin to work together towards a common goal—behaviours, beliefs and attitudes will change. Once this occurs, these behaviours will be passed on to new generations of employees as norms and rules. This is when true change can be seen.

While it sounds like a daunting task (and it is), changing the DNA of the enterprise is possible. The benefits of creating a culture that is conscious of and conducive to security apply not only to the security manager but also extend to the enterprise; its partners; and, most important, its customers.

---

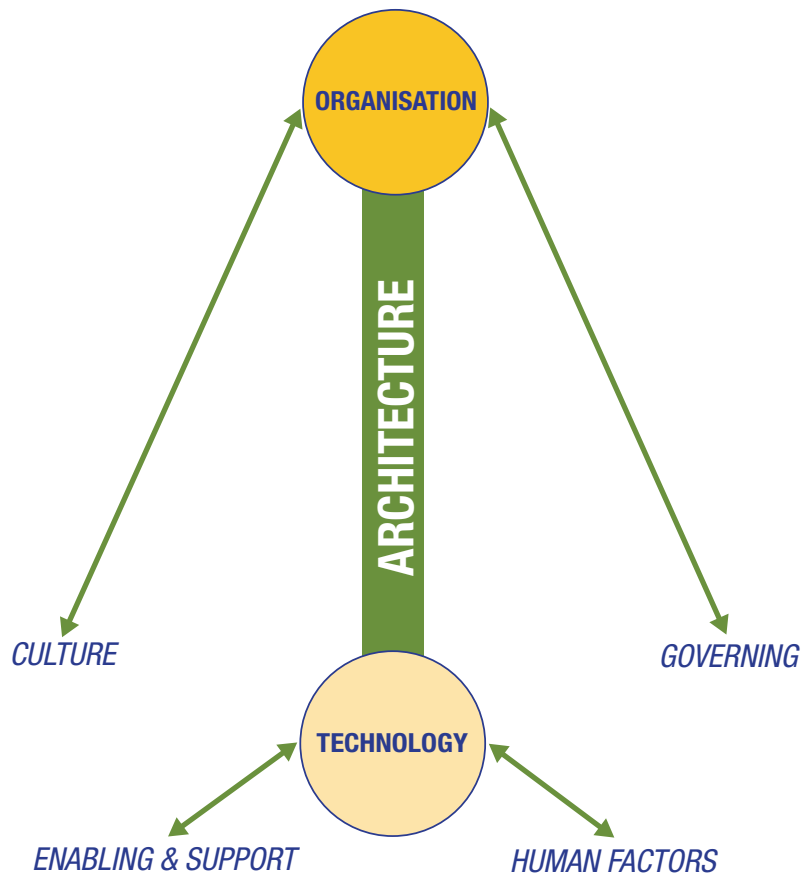
<sup>25</sup> Deal, Terrence E.; Allen A. Kennedy; *Corporate Cultures: The Rights and Rituals of Corporate Life*, Boston: Addison-Wesley, USA, 1982

# THE BUSINESS MODEL FOR INFORMATION SECURITY

## Architecture

Architecture (**figure 10**) is the DI that connects the elements of Organisation and Technology. While architecture is often equated to infrastructure when dealing with security or IT, it is important to note that architecture constitutes much more than that. In many respects, the information security architecture is analogous to the safety and security architecture associated with buildings.

Figure 10—Architecture DI



Architecture begins as a concept, a set of design objectives that must be met (e.g., the function it will serve; whether it will be a hospital, a school, etc.). It then progresses to a model, a rough approximation of the vision forged from raw materials (services). This is followed by the preparation of detailed blueprints, tools that will be used to transform the vision/model into a real and finished product. Finally, there is the building itself, the realisation or output of the prior stages. According to ISACA's *CISM Review Manual*:

*The underlying notion for all architecture is that the objectives of complex systems must be comprehensively defined; have precise specifications developed; have their structures engineered and tested for form, fit and function; and have their performance monitored and measured in terms of the original design objectives and specifications.*<sup>26</sup>

ISO/IEC 42010:2007 defines architecture as:

*The fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.*

A number of specific approaches to security and enterprise architecture exist, which can generally be categorised as either frameworks or process models. If an enterprise architecture includes the organisation's security objectives, it inherently sets the scene for the detailed security architecture. However, separating the security elements from the overall architecture does not help integration, which is the overarching aim of BMIS. While a number of approaches to enterprise and, specifically, security architectures are available, one of the most common is The Open Group Architecture Framework (TOGAF). Another widely accepted approach is the Zachman enterprise framework<sup>27</sup> and the derivative Sherwood Applied Business Security Architecture (SABSA) security framework.

<sup>26</sup> ISACA, *CISM Review Manual 2011*, USA, 2010, section 3.13.2, Objectives of Information Security Architectures, p. 178

<sup>27</sup> [www.zachmaninternational.com](http://www.zachmaninternational.com)

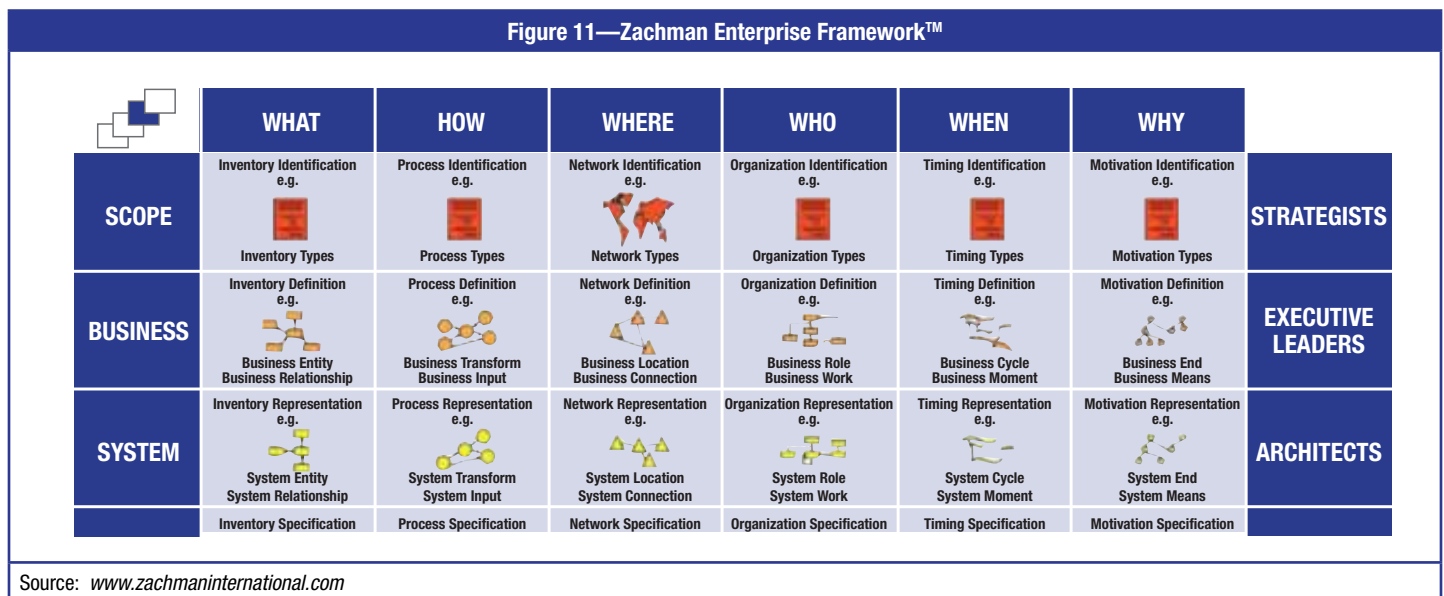


## 2. BUSINESS MODEL FOR INFORMATION SECURITY

Since BMIS is a model encompassing a number of broad areas, the first steps in utilising it must be simple and straightforward. As a result, for the purposes of this document the broadly inclusive and readily applicable Zachman framework for enterprise architecture is a good starting point. This framework adds to BMIS by providing defined levels of architecture and components within these levels.

In the Zachman framework, each element is shown in relationship to the higher-level, less detailed aspects and to the levels below at greater granularity. The six-layer hierarchy is shown as contextual, conceptual, logical, physical, component and operational. Each layer shows the relationships and interactions of its components. The top layer (contextual) is connected directly to organisational design, while the physical, component and operational layers link to the Technology element.

Beyond the somewhat abstract ISO definition, architecture in the functional, inclusive sense might best be described as a grouping of related designs from different perspectives at various levels of detail. For BMIS, only the top three levels of the Zachman Enterprise model need be considered, as shown in **figure 11**.



The highest (contextual) level defines the relationship of a structure to its surroundings. In terms of a building, this would be equivalent to a rendering of the building in its surroundings with roads, parking lots, trees, etc. The same notion applies to information security. It resides within the context of the organisation, and contextual architecture will describe its relationship to the organisation: where in the structure it exists—its relationship to other organisational entities such as finance, legal, marketing and/or operations.

At this level, the Architecture DI exists to make sure that business information security complies with the laws and regulations of the country as well as industry sector specifics, including the expectations and requirements of customers or partners. In addition, information security standards that are viewed as best practice may be considered. The Architecture DI also supports organisational strategy in recognising strategic objectives and their implications for the information security architecture and technology solutions.

The next level down, below the contextual architecture, is the conceptual level, which is the building equivalent of the exterior of a building from various perspectives referred to as elevations. For information security, this will define what the overall function looks like, its dimensions and scope. It will indicate points of ingress and egress (doors) and points of visibility (windows).

The conceptual level for information security ensures that technology (physical and logical) will not just support, but actively enable, the security objectives. This level holds a set of interrelated, co-operative and integrated security activities and technologies that work towards achieving a common security objective.

The next (logical) level of architecture for security is similar to the floor plan of a building. It shows the internal relationships and the activity flows amongst them.

The logical level specifies the more detailed design of the security components, using technology to make sure they will achieve the defined objectives, be resistant to attacks and even sustain damages. At the logical level, the overall architecture blueprint is created that gives a sense of direction to technology-side management and clearly outlines what to do. It also aims at ensuring that the output of one security technology is appropriately communicated (in time and format) to the other technologies that use it, providing the most effective and efficient feedback of the security process on technology and achieving its final objective without undue delay.

# THE BUSINESS MODEL FOR INFORMATION SECURITY

However, security and technology architectures depend not only on business objectives, but also on the general information architecture. Information flows from one point of the enterprise to another must be considered in detail. In addition, information storage and retrieval are an intrinsic part of security architecture.

The concepts and considerations of a building architecture must also be included in the security aspects of an enterprise architecture. These include elements such as the capability of expansion (scalability) and usefulness for a variety of purposes (adaptability). Enterprise architecture must include and allow for:

- **Space for evolution and improvement**—Architecture must allow for the inevitable changes in the organisation and its activities as well as for upgrades and improvements over time. Additionally, when technology brings new possibilities, architecture will feed the organisation design and strategy to provide the incentive for an evolution that may have been put in a waiting state, both conceptually and logically.
- **Space for reaction to changes in context**—The context is the business landscape within which the architecture operates. The context will inevitably change. Adaptability, resilience and robustness are attributes that must be considered and included in design activities. Architecture ensures that the technology will resist changes, just as a building is resistant to attacks or earthquakes. If Architecture can feed Organisation with some specific features of technology to support or become stronger from events, this will enhance the reaction capacity of the business to follow the proposed, required or imposed (e.g., due to crisis) changes.
- **Fitness for purpose**—Technology implementations often fail to meet business requirements because the context was not understood or was ignored. Just as building architecture must consider whether it is to be used as a church or a tuna canning facility, enterprise architecture must clearly understand the business objectives that technology will be used to realise. The more technology is fit for purpose, the higher the chance that business security objectives will be supported/enabled by an appropriate technology.
- **Effectiveness and efficiency**—Effectiveness and efficiency in information security require related technology solutions to be equipped with the indicators that measure status and achievement of expected objectives. Costs associated with the use of technology for security are also taken into account by architecture: acquisition, implementation, operation, monitoring, maintenance and management. Cost is a combined set of all resources involved: finance, time and people.
- **Consistency with policy and standards**—Architecture must articulate policy in addition to addressing business requirements. Architecture ensures that technology remains consistent with policies and standards, and helps keep technology solutions updated through the Enabling and Support DI. If technology solutions were to prevent or hinder the achievement of the objectives of policies and standards, this would create a serious issue that Organisation would have to resolve. Convergence, coherence and consistency amongst all security components (the three other elements and the five other DIs) are critical objectives for ensuring the effectiveness and efficiency of the security plan and its management.
- **Maintainability and usability**—Good design must consider how systems will be developed and maintained over time. Technology, if unchanged, will rapidly age and become obsolete. As a result, maintenance must be planned into the Architecture DI. After a given period of time, both preventive maintenance (to prevent degradation and obsolescence) and *ad hoc* maintenance (in unforeseen situations) is required to adequately develop the Technology element.

---

**Architecture must ensure that progress is built into the system to adapt to evolving demands.**

---

Since technology must remain usable—and easy to use so people are not hindered in their day-to-day security activities—the Architecture DI must ensure that progress is built into the system to adapt to evolving demands.

In BMIS, Architecture is the DI between Organisation and Technology. The interaction between these elements is bidirectional, each influencing the other. The organisational design and its business strategy provide the drivers and constraints through the Architecture DI to IT and physical operation environment. These include:

- **Size**—The scope and charter of technology security are functions of organisational design and business strategy. In security, size represents the part or proportion that each technology will provide in achieving the security objectives while remaining current.
- **Capacity (static and dynamic)**—Operational capacity of the technology solutions is an important function of business security requirements. Capacity planning for future operations is, in turn, a function of the business strategy and anticipated requirements. This relates to physical capacity planning and logical capacity planning.
- **Roles and responsibilities**—Roles, responsibilities and operational activities are defined in the architecture as a function of organisational design and anticipated business requirements. Technology must also ensure that information security supports the segregation of information when and where needed, so that business roles and functions are not contradictory.
- **Centralised and decentralised operations**—Architecture must take into account the shape and structure of the overarching organisation. In terms of security, centralised (hierarchical) structures vary significantly from decentralised (flat) organisational structures and require a different security architecture.

The technology solutions applied should follow the business requirements. This includes physical co-location, decentralised work and telework, and *ad hoc* working groups that form at infrequent intervals. The routing and firewall infrastructure is a good example: in a strongly decentralised organisational structure, there is a more pressing need for flexibility in switching, routing and firewalling.

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

Conversely, technology security may enable the centralisation of secure operations, even when the physical locations are geographically spread, sometimes in different countries or on other continents. Examples of a virtual centralisation strategy expressed in the security architecture are virtual private networks (VPNs) across wide area networks (WANs) or public networks, secure video conferences, and secure darknets.

- **Quality and security needs**—The organisational architecture determines the requisite minimum level of quality of security services (QoSS) and design parameters of security controls, including policy. The Organisation element identifies desired quality levels on the basis of business requirements and security objectives, which are then reflected in technology solutions. Again, architecture translates organisational objectives into the ‘right’ technology, and it informs technology in terms of the required quality of service.

The Technology element must provide feedback and influence the Organisation element in the form of measures and metrics. Some of the major influences on organisational design and strategy include:

- **Cost and value**—What is the cost (acquisition, implementation, operation, management, maintenance) of security technology? What is the added value of information security technology to the business in enabling set objectives?
- **Capability**—Is technology capable of providing the required security service? When will that be possible? What can be done to reduce the time to achieve full capability?
- **Agility**—Will Technology be agile and versatile enough to follow changing security demands of the Organisation, Process and People? How fast should these changes happen? Are there time windows in the life span of technology solutions when changes will be more difficult or easier to accomplish?
- **Availability**—Business requires connectivity and constant availability of information. While security has a responsibility to protect information, it also has a responsibility to ensure that information is available to those who are granted access when they need it. How can technology provide solutions to allow for secure interconnectivity, where and when needed? What security trade-offs would then be acceptable, if any?
- **Complexity**—Information and communication technology does not always use standard solutions, thus creating complexity. A similar issue exists in the physical environment—the other side of technology—when decentralisation or acquisitions require the use of various buildings with divergent security solutions. The Architecture DI provides the link between what merging or acquiring organisations set as their objectives, and the integration of divergent technologies that may be found in the targets.
- **Space and energy requirements**—Technology needs controlled space and sufficient energy to operate. This is frequently a burden when there is a need to increase the size and capacity of IT. In terms of security, the physical environment creates a number of challenges—for instance, where there are links to public infrastructures or where the secure facility depends on outside services. An example is the frequent lack of electrical power (wattage) that often restricts data centre operations. Likewise, the coupling of pure IT security with ‘in-between’ technology such as facilities management, field bus installations or HVAC often create the need for specific security measures.
- **Architecture considerations**—These include how an organisation reacts to direct technological changes or to indirect technological changes caused by the external environment.

Architecture should proactively transmit any information on direct technological changes to the organisation element, both in terms of what the change is and what the change means for the business. Similarly, architecture should inform the organisation about indirect changes that may be triggered by the environment of the firm, such as major updates or release changes in key applications. Information security depends on the regular and accurate feedback that originates from the Technology element and is processed within the Organisation element, thus leading to informed decisions.

- **Architecture and risk considerations**—While people, process and technology have long been accepted as the management triad for IT, there are many security risks that stem from day-to-day imperfections, flaws and errors in the overall system. Since most systems do not always run in ‘flawless’ mode, the security architecture must be sufficiently resilient to accommodate anomalies, incidents and errors.

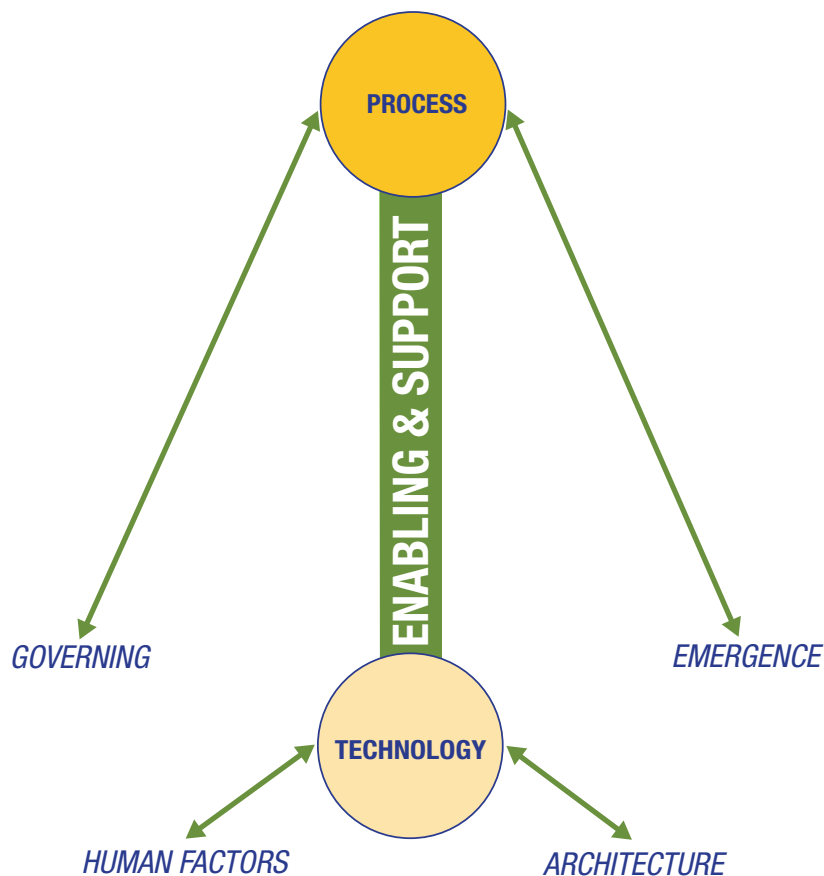
Some of the least addressed issues that must be taken into account in the risk assessment are delays inherent to technology, the inability of technology to fully implement security objectives, and the requirements of technology to appropriately host and perform business activities and security processes while remaining easy to use.

- **Security architecture**—This provides a balanced relationship between strongly opposing elements and the interplay of conflicting elements, and serves as a device for regulating tautness amongst an organisation’s governance, technology architecture and operations. Architecture should enable the organisation to understand the balance between too much security technology and too little of it. As a secondary task, the security architecture is the decisive factor in balancing ‘tautness’, i.e., the responsiveness of organisational decision making to technology changes and *vice versa*.

### Enabling and Support

The Enabling and Support DI connects the Process and Technology elements. In BMIS terms, it is the dynamic interconnection through which technology enables process, and process in turn supports the deployment and operation of technology, as shown in figure 12.

Figure 12—Enabling and Support DI



As the Enabling and Support DI is the area that demonstrates a balanced process to support the enterprise technology in one direction and show the effect technology has on business processes in the other direction, it is helpful to look at a few examples.

There are plenty of examples to illustrate the fact that in the absence of a balanced process that supports technology, IT solutions fail to meet the business objectives and become liabilities. To recognise problems before they surface, some ‘detective measures’ must be in place. However, in a weak Enabling and Support DI subsystem, such support measures are likely to be absent or ineffective.

A strong Enabling and Support DI should take into account:

- Balanced processes and quick adjustment to a new equilibrium state
- Adherence to appropriate standards
- Use of appropriate controls
- A strong security focus
- Recognition of compliance requirements

Most important, the Enabling and Support DI system has to generate the desired return on investment (ROI) and meet the business objectives.

With most enterprises going through numerous audits and compliance reviews annually, reliance tends to be on those audits and reviews targeting the effectiveness of processes and IT infrastructure security. That trust is not misplaced, but organisations must look beyond audits and compliance reviews and take stock of their processes around the use of technology.

This means that organisations must first understand the relationship between the Process and the Technology elements. This DI has been named Enabling and Support in BMIS with the view that process enables technology and technology supports the business process.

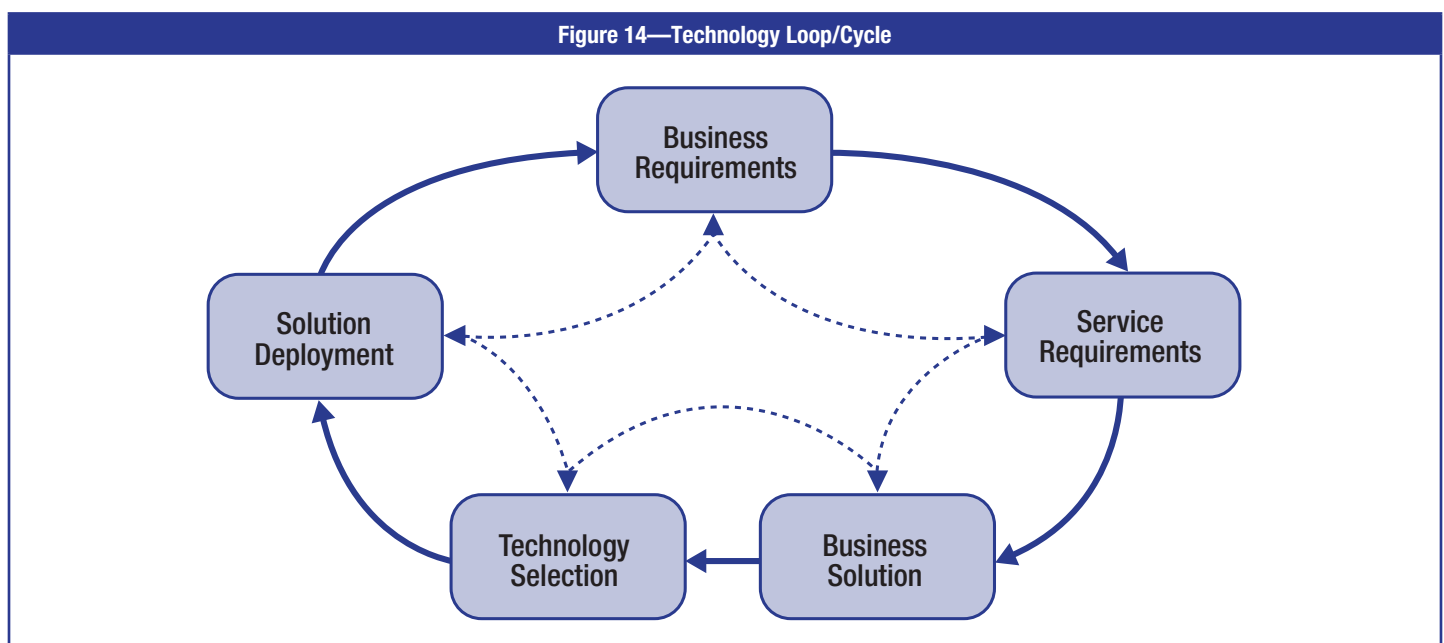
Technology needs to be selected, evaluated, implemented and controlled. Processes have to be designed, developed, implemented and utilised. The difficulty that most organisations struggle with is not a lack of technology; processes are often insufficiently enabled by existing technology, while the abundance of technology within any organisation is inadequately supported by existing processes.

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

Many organisations focus more on the technology itself than on understanding the business process that the technology will enable. Their view of the technology is linear, as illustrated in **figure 13**.



This process map is straight and sequential, with no feedback loop or ‘do-overs’. Once the technology is acquired, the organisation generally utilises vendor support for its implementation. Organisations sometimes reduce or remove vendor support without having a fallback process in place. Knowledge transfer and documentation are ignored in favour of fixing the problems and making the technology work in a hands-on mode. In systemic thinking, the linear model does not resolve any of the problems that arise from sequential technology implementation and maintenance. As a consequence, the BMIS way of thinking favours a loop, as depicted in **figure 14**.



The loop allows going back to previous steps as required to systemically adapt any of the steps in the cycle. For instance, if the technology solution appears unclear or insufficiently defined, the business solution is revisited to ensure alignment. If the business solution is unclear or raises questions, it may be necessary to go back to the original service requirements formulated or even to the overarching business requirements. However, this is not a step-by-step sequence as shown in **figure 13**. It is systemic in that no step in the loop is ever ‘completed’, but all steps interact in the overall cycle and may change the technology solutions and their deployment.

When technology selection and implementation are part of deploying a business solution, there is a cyclical process that enables appropriate solution components to play a role. BMIS helps ensure a holistic and balanced view of technology enablement. The model does not advocate state-of-the-art technology or complete automation, but instead focuses on enablement of the business by the use of technology.

Processes are ways of achieving objectives. Without objectives, processes are not measurable and are of little use. The same applies to technology (the object), which has no value if it does not allow the organisation to achieve its goals in implementing its strategy (even if this strategy evolves).

It follows that there is a co-dependency between the Process and Technology elements that makes it difficult to isolate one from the other. The Enabling and Support DI is a tightly coupled two-way relationship that can be understood only when the three building blocks of systems thinking (feedback, equilibrium and delay) are applied, as outlined later in this section.



## IT Within an Enterprise

In his article 'Information System Integration', Wilhelm Hasselbring<sup>28</sup> describes the fragmentation of information systems within enterprises. According to the researchers, most security failures result not from a lack of standards and technologies, but from a lack of approach in utilising them properly for the benefit of the entire organisation. Upon uncovering a security flaw—due to an incident or as the result of an audit—organisations rush to fix the flaw, sometimes without understanding the root cause or correlating it to similar flaws discovered before.

### Example

If a file containing US Social Security numbers (SSNs) is sent out unencrypted and against the organisational policy, chances are that the organisation will establish a new practice and ask its employees to encrypt the files—because that is the common practice today.

While this may work in some cases, it has its own flaws since people do not always follow the process and the possibility that the SSNs could be sent in the clear would still exist. Furthermore, there may be other modes of data transfer where data are being transmitted in clear text. Obviously, the issue then will be much broader than just the e-mail security. Hence, organisations need to consider a different approach to solving problems and developing solutions, which BMIS provides.

In the previous example, the systems approach of BMIS will cause the organisation to take other factors into account before settling on 'the solution'. For instance, an organisation adhering to BMIS concepts may consider the following questions:

- Before we implement e-mail encryption, are processes well defined and strictly followed? If not, what is the probability that the new process (to encrypt files) will be followed as intended?
- Are people/resources available to help answer questions or resolve problems as a result of this new process? Are employees educated in protecting sensitive information? Do they understand why this information must be protected?
- Is the proposed encryption technology easy to use? Does it require a great deal of manual intervention?

From an organisational perspective, other questions may be asked:

- Is this the best solution? The best cost solution? Is it a short- or long-term solution? What are the alternatives? What similar problems have been encountered? What future problems will this present? What is the cost of compliance? How would customers react to the solution?

The questions in the previous four bullets represent the BMIS elements. Breaking questions down by element helps achieve a balanced solution by further analysing the answers within the context of the dimensions of BMIS:

- Processes are well defined; however, the organisation lacks trained people to support them.
- Encryption has been tried before; however, the organisation culture tends to be very informal and people send unencrypted e-mail when they think they can 'trust' the other party.

BMIS thus enhances an organisation's ability to relate critical influencing factors, and as the organisation considers Culture, Architecture, Human Factors, Governing, and Enabling and Support issues, management may decide to eliminate (mask) SSNs from file extracts, thereby eliminating the risk altogether.

As most information systems tend to be autonomous and operate within their own silos, the process of feedback either does not exist or exists at a layer that does not filter down to the level of enabling and support. **Figure 15** shows how most organisations operate.

These siloed organisational units tend to focus more on the technical architecture than on the structure, as described earlier in this section. This is one of the underlying root causes of the failure to utilise technology to meet business objectives.

However, if organisations allow integration of silos, a different outcome can be observed (**figure 16**).

It is evident that integrated organisational processes could lead to better enabling results as well as to better support.

Integration across organisational units is not a trivial task. When an organisation recognises a deficient Enabling and Support DI environment, it tends to focus on one or more of the following factors or resources:

- **Technology**—Current technology does not permit meeting the business objectives; hence, new investments must be made to acquire newer technology.
- **People**—There is a lack of management skills, people resources, knowledge, motivation or commitment.
- **Culture**—Historically, this is how things have worked, so it cannot be changed.

<sup>28</sup> Hasselbring, Wilhelm; 'Information System Integration', *Communications of the Association for Computing Machinery (ACM)* - CACM, USA, 2000, vol. 41, no. 12, p. 64-70

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

Figure 15—Organisational Fragmentation

### Non-integrated Vertical Organisation Structure

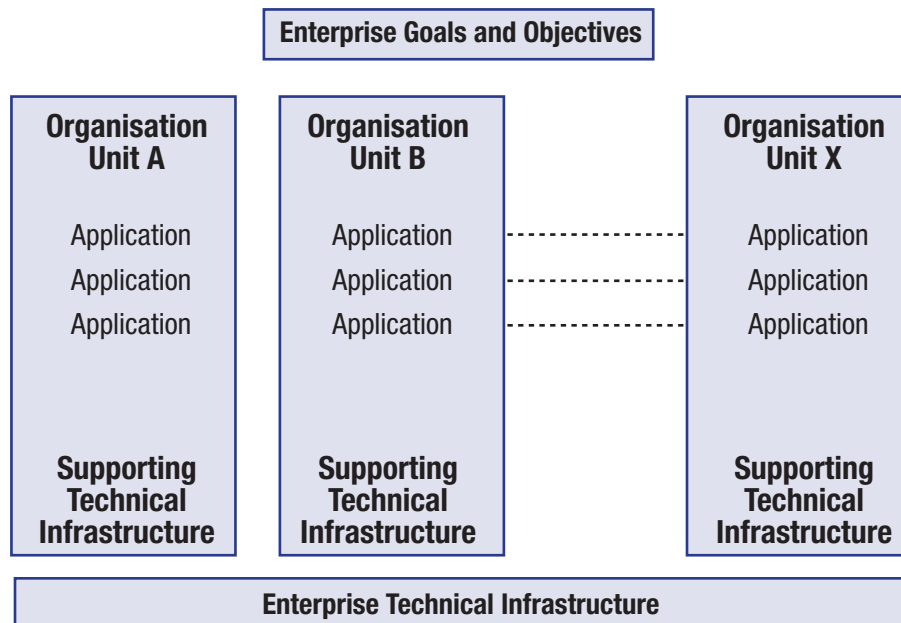
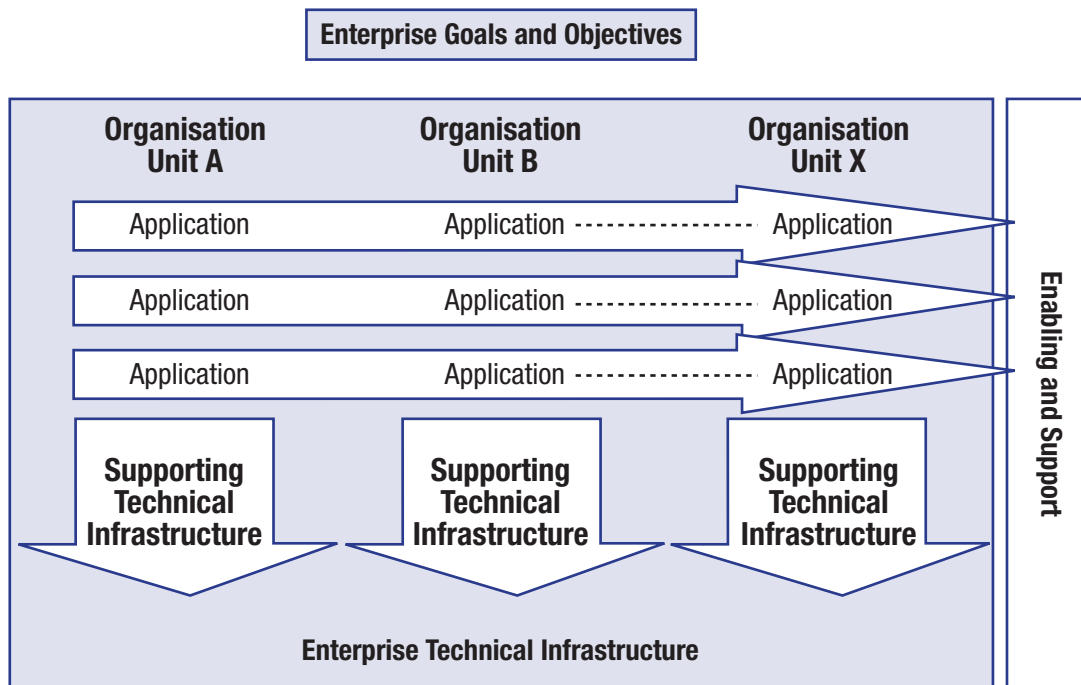


Figure 16—Organisational Integration

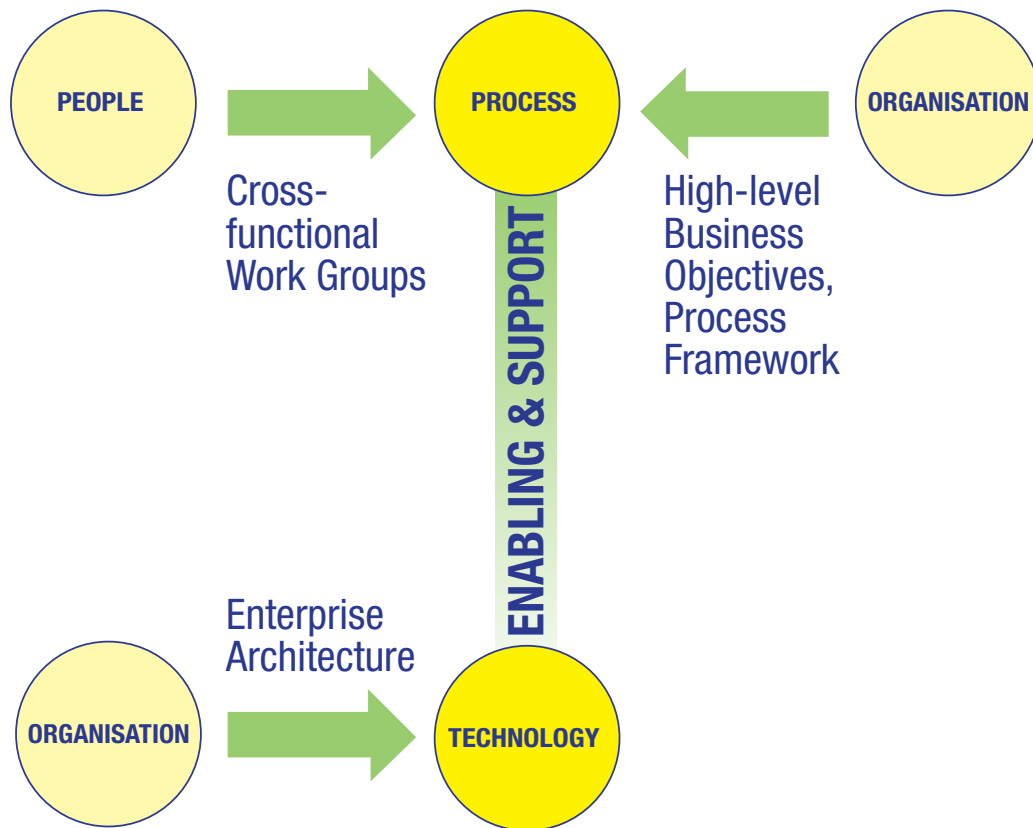
### Integrated Vertical Organisation Structure



# THE BUSINESS MODEL FOR INFORMATION SECURITY

In many organisational cultures, people avoid highlighting problems until something drastic happens. This is where BMIS, with its systems approach, helps. Identifying and focusing on all of the factors that may contribute to the problem can result in action plans that not only help solve the problem, but also establish a road map for proactively implementing an effective Enabling and Support DI infrastructure. This road map will differ from organisation to organisation, but it is likely to have the key components shown in figure 17.

Figure 17—Key Components of the Enabling and Support DI Infrastructure



The key components of the Enabling and Support DI infrastructure are:

- **High-level business objectives**—Information technology is a business enabler in that it helps reduce operating costs, improves productivity and generates new growth. Implementing a new accounting system or marketing plan is not likely to generate long-term growth or reduce costs across the entire organisation. Businesses must undertake enterprise-wide initiatives to achieve broad, general business goals such as reducing costs,<sup>29</sup> which is the ultimate goal achieved by the Enabling and Support DI.
- **Detailed business requirements**—Business requirements are the detailed set of business requests that the system must meet to be successful.<sup>30</sup> Business requirements should be gathered without reference to technology. Gathering business requirements is a critical activity even if the project focus is a technology upgrade or refresh.
- **Enterprise architecture and process frameworks**—The plans and goals of the technology must align with the plans and goals of the organisation.<sup>31</sup> For that to occur, key functional areas and processes, along with their information-sharing needs and service consumption/delivery, need to be aligned and integrated. The vehicle to accomplish this is enterprise architecture.

According to P. Baltzan and A. Phillips, ‘companies building a foundation for execution should use their enterprise architecture as a compass, directing the company toward its intended operating model’.<sup>32</sup>

Enterprise architectural processes ensure vertical and horizontal integration, provided the detailed business requirements have been considered and documented. A good example is the process of identification and authentication within an organisation. Unless the technological Identity Access Management (IAM) solution is integrated within all parts of BMIS, the result will be incomplete and

<sup>29</sup> Baltzan, P.; A. Phillips.; *Business Driven Information Systems, 2<sup>nd</sup> Edition*, McGraw Hill, USA, 2008

<sup>30</sup> Ibid.

<sup>31</sup> Ibid.

<sup>32</sup> Ross, J.W.; P. Weill; D.C. Robertson; ‘Enterprise Architecture as Strategy—Creating a Foundation for Business Execution’, Harvard Business School Press, USA, 2006, p. 11



## 2. BUSINESS MODEL FOR INFORMATION SECURITY

vulnerable since employees who have left the organisation will still be able to access critical information—a perennial problem. However, there is enough evidence to prove that many organisations have bought the technology without considering the overall organisational view. Furthermore, they have not considered integration of this technology from a support perspective, such as who is going to handle user calls for help or how the technology will integrate with the legacy systems. All too often, organisations listen to the vendor and assume that the product will somehow understand and meet their needs out of the box.

- **Cross-functional work groups**—Having cross-functional work groups overseeing the items mentioned in the three previous bullets is essential to establish a successful Enabling and Support DI structure. Rather than one or two people trying to understand the entire enterprise, it is advisable that members of various organisation units come together to establish business objectives, understand business requirements and develop an enterprise architecture. Even in a situation where such an architecture exists but is ineffective, it is critical to set up a cross-functional work group to diagnose the problem and recommend a solution.

There are other reasons to create cross-functional teams. A strong Enabling and Support DI that incorporates multi-disciplinary views contributes to better security by eliminating redundancies and fostering greater communication. There is another aspect that also should be considered:

*...Computers have to interact with users in some way, at some time, for some reason. And this interaction is the biggest security risk of them all.<sup>33</sup>*

---

**A strong Enabling and Support DI that incorporates multi-disciplinary views contributes to better security by eliminating redundancies and fostering greater communication.**

---

Cross-functional teams can provide valuable input to the enterprise risk management process by sharing their own experiences, both good and bad. For example, people like the fact that they may not have to enter passwords on every screen they enter. Enabling and Support DI systems foster security of the technology while keeping processes user-friendly (for instance, through the introduction of a single sign-on mechanism). Human factors are an essential ingredient to the Enabling and Support systems.

### Emergence

On hearing the term ‘emergence’, concepts that come to mind may include surfacing, developing or evolving. In previous business models it might have been called ‘continuous improvement’. Peter Senge calls this ‘learning’.<sup>34</sup> Another definition of emergence is ‘the arising of novel and coherent structures, patterns and properties during the process of self-organisation in complex systems’.<sup>35</sup> In BMIS, emergence can be seen as the arising of new opportunities for business, new behaviours, new processes and other security-relevant items, as the subsystems between people and processes evolve (**figure 18**). The ‘learning’ aspect stems from the fact that even seemingly chaotic systems, as in fairly new organisations or unforeseen situations, tend to develop some form of order. Emergence in biology and cybernetics sometimes creates ‘order out of chaos’<sup>36</sup> in an unpredictable way.

Emergence as such does not always signal improvements in terms of security. As spontaneous new ways of doing things emerge within an organisation, they may be positive or negative. For instance, habitual behaviour that is counter to policies and standards may evolve over time. Likewise, the level of security may improve through people’s tacit agreement on how to handle new systems or applications. The way in which People (as a BMIS element) interact with processes is often characterised by Emergence, making it a very powerful DI. It is an area that addresses ambiguity and evolution and, if managed well, can improve the enterprise’s ability to adjust to change, survive an unanticipated event and innovate.

---

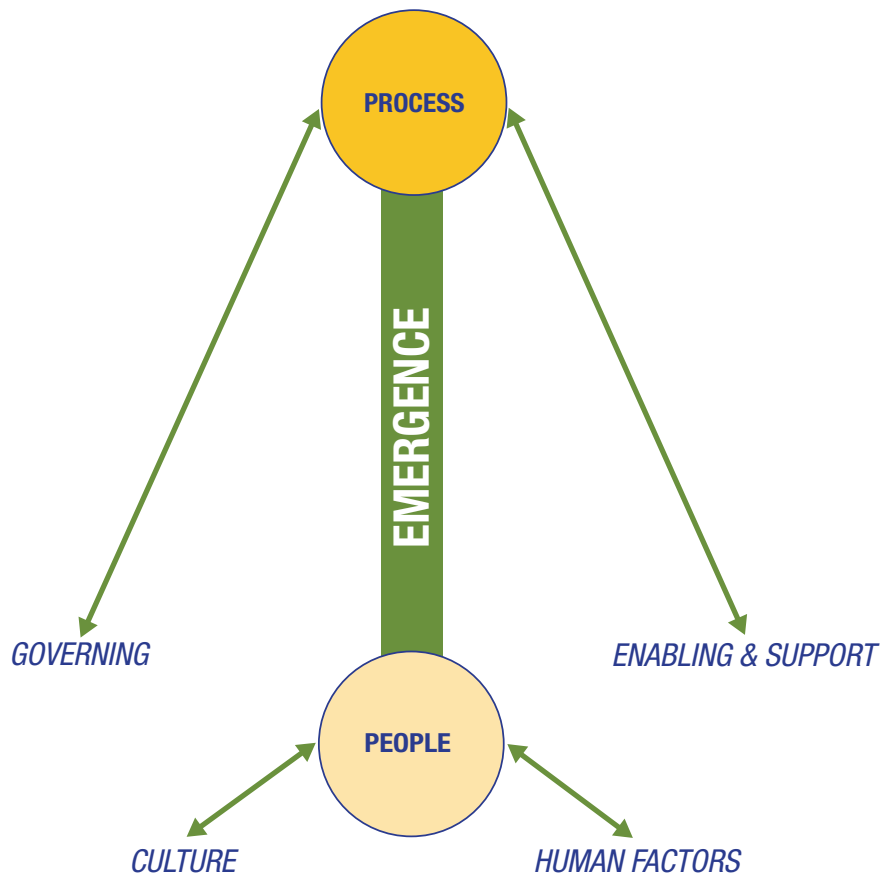
<sup>33</sup> Schneier, Bruce; *Secrets and Lies—Digital Security in a Networked World*, Wiley, USA, 2000

<sup>34</sup> Senge, Peter; *The 5<sup>th</sup> Discipline, The Art and Practice of the Learning Organization*, Currency Doubleday, USA, 1990

<sup>35</sup> Goldstein, J; ‘Emergence as a Construct: History and Issues’, [http://iscepublishing.com/\(X\(1\)S\(0hxda5554vqewgzy2m4uihzt\)\)/ECO/eco\\_papers/issue1\\_1\\_3.pdf](http://iscepublishing.com/(X(1)S(0hxda5554vqewgzy2m4uihzt))/ECO/eco_papers/issue1_1_3.pdf), 1999, p. 49-72

<sup>36</sup> Prigogine, I.; *Order Out of Chaos*, Bantam Books, USA, 1984

Figure 18—Emergence DI



## Understanding Emergence

Human nature dictates that the execution of processes by people within an enterprise varies over time and every time a process is executed. A process in itself can be well defined, but its outcome may be different each time it is executed. This means that only part of the process is predictable, whereas other parts may have an element of coincidence. To be able to understand the impact of this fact on information security, the execution of a process by people is subdivided into the following categories:

- **Written procedure-based**—The execution of tasks based on the specific flow of actions defined in an official procedure
- **Policy-based**—The execution of tasks based on the translation of rules of the enterprise security policy
- **Ad hoc**—The execution of tasks in a random manner, not covered by a procedure or policy rule

Each execution category contains different elements of uncertainty as introduced by the basic characteristics of human nature—the ability to think, decide and react in various situations:

- **Written procedure-based**—People may or may not comply with a procedure; they may make mistakes when following a procedure or misunderstand it. The procedure itself may not be appropriate for covering all possible situations, or it may be very difficult and confusing to follow. In some instances, several people may decide—without knowing what the others are doing—to interpret written procedures in a similar way. As a result, a new way of handling the procedure emerges.
- **Policy-based**—Rules are more general than a specific procedural flow. They may be translated differently in distinct situations, mistranslated or ignored. The rules may be too strict or too general, correspondingly being inapplicable in time-critical situations or providing too many alternatives, thus not serving the scope of information security.
- **Ad hoc**—Uncertainty is maximised when people are not instructed to follow procedures or rules for executing processes since behaviour is not placed in a specific framework.

The concept of emergence comes from many different fields, including systems theory, game theory and nature itself. Chaos theory also explains the concept of emergence to an extent. In chaos or decentralised or leaderless situations, some type of order may emerge or surface in a seemingly spontaneous way and without obvious cause. Similarly, people may individually decide to adopt new technologies or processes—for example, when they are using IT at home in a different way from how it is used in the workplace. The motivation for people to do so may lie in human factors and convenience of use or in a cultural background that influences their behaviour. In BMIS, Emergence is the DI between the People and Process elements. However, anything that people think or do must take into account the other DIs that influence People: Human Factors and Culture.

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

Emergence, as a learning process, is critical for information security since it assists in understanding the requirements for shaping effective security strategies that fit the behaviour of the enterprise as a whole. It helps in customising, improving and expanding security procedures and rules to bring information security from theory to practice. It is a time-consuming process that requires an environment of free expression in which people are able to provide feedback that contributes to making security a business enabler that does not impede performance, but rather helps better organise the execution of processes. To ensure strong security in organisations, there must be a level of preparedness and a climate of ‘having covered all bases’ in terms of the People, Organisation, Process and Technology elements. The system of rewards and incentives should not favour only the preservation of old processes, but also actively encourage the development of new processes and ways of doing things and identification of problems before they arise in practice.

**Emergence, as a learning process, is critical for information security.**

**Emergence** can be classified as *positive* or *negative*. Positive emergence is related to the learning process for understanding security needs and improving information security. Negative emergence is related to the increased phenomenon of unexplained security incidents and lack of alignment between information security and business goals.

Therefore, the Emergence DI introduces an element of evolution and accommodates the sometimes unexpected, or even unpredictable, changes that occur in day-to-day business. As a concept, it further enables business to anticipate such changes and integrate them into the overall security system and its subsystems.

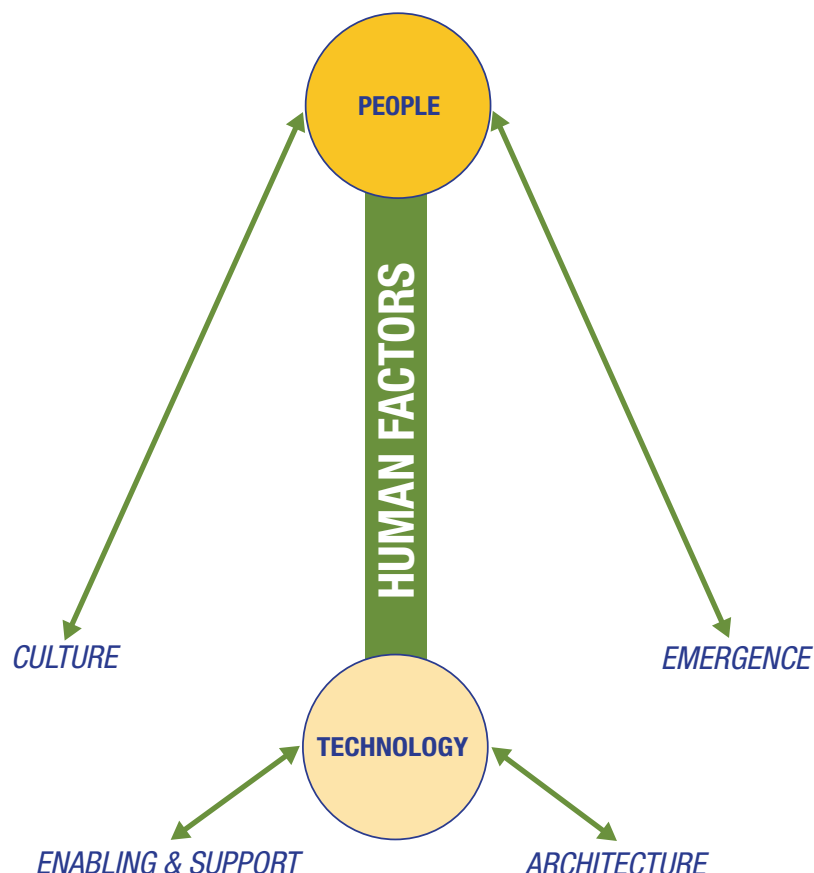
### Human Factors

Human Factors is the DI that connects the elements of People and Technology. Human Factors is an extensively documented field that covers many areas such as the:

- Science of understanding the properties of human capability, ergonomics and boundaries of human skills
- Application of this understanding to the design, development and deployment of technologies and services
- Art of ensuring successful application of human factors engineering to a programme

The Human Factors DI (**figure 19**) has been referred to as human-computer interaction (HCI), the man-machine interface and ergonomics. In practice, much of the work on user-friendliness and usability relates to this DI.

Figure 19—Human Factors DI



**Weaknesses in security can easily occur due to the way in which people use technology and their understanding of the need for and adherence to security concepts.**

The Human Factors DI also includes the study of how humans interact with technology and the development of tools that facilitate the achievement of specific goals—in this case, information security objectives. Within BMIS, the Human Factors DI interacts with the People and Technology elements. This relationship follows from the fact that weaknesses in security can easily occur due to the way in which people use technology and their understanding of the need for and adherence to security concepts. Similarly, Technology as an element can greatly enhance the quality of work and the way in which people accomplish their tasks.

In general, the three main objectives within the Human Factors DI relate to the human operator (body and mind) and the surrounding systems that interact with the human user. To understand and manage tension in this DI, the first step is to diagnose or identify the problems and deficiencies in the human-system interaction of an existing security system. Subsequently, there are five different approaches that can be utilised to introduce improvements:

- **Equipment design**—Changes the nature of the physical equipment with which humans work
- **Task design**—Focuses more on changing what operators do than on changing the devices they use. This may involve assigning part or all of tasks to other workers or to automated components.
- **Environmental design**—Implements changes such as improved lighting, temperature control and reduced noise in the physical environment where the task is carried out
- **Training the individuals**—Better prepares employees for the challenges they will encounter in the job environment by teaching and practicing the necessary physical or mental skills
- **Selection of individuals**—A technique that recognises the individual differences amongst humans in every physical and mental dimension that is relevant for a good system performance. Such performance can be optimised by selecting operators who possess the best skills profile for the job and selectively strengthening certain skills across teams.

The simple People-Technology model consists of a person interacting with a ‘machine’ in some type of environment. The person and machine/environment are both modelled as information-processing devices, each with inputs, central processing and outputs. The inputs of a person are the senses (e.g., eyes, ears) and the outputs are effectors (e.g., hands, voice). The inputs of a machine are input control devices (e.g., keyboard, mouse) and the outputs are output display devices (e.g., screen, voice alerts).

The environment can be characterised physically (e.g., ambient temperature, noise, closed environment), cognitively (e.g., time pressure, awareness and understanding, risk) and/or organisationally (e.g., organisational structure, management involvement). This provides a convenient way for organising some of the major concerns of human factor engineering: the selection and design of machine displays and controls; the layout and design of workplaces; design for maintainability; the design of the work environment and, in particular, the security infrastructure.

As an example, driving a vehicle is a familiar example of a simple man-machine system. In driving, the human receives inputs from outside the vehicle (e.g., sounds and visual cues from traffic, obstructions and signals) and from displays inside the vehicle (e.g., the speedometer, fuel indicator and temperature gauge). The person continually evaluates this information, decides on courses of action, and translates those decisions into actions upon the vehicle’s controls—principally the accelerator, steering wheel and brakes. Finally, the driver is influenced by environmental factors such as noise, fumes and temperature.

The study of ergonomics has its origins in the Industrial Revolution and emerged as a full-fledged discipline during World War II. It was recognised that aircraft cockpit design needed to consider the human interface for controls and displays. Design engineers focused on the technology and industrial psychologists worked to optimise the interface. In some cases, human factors design can affect bottom-line profitability or can be a life and death matter—for example, in designing interfaces in high-risk industries. Companies came to realise that the success of a product is dependent upon good human factors design.

People work best and make fewer mistakes (potentially reducing the security risk) when they are in a familiar environment. Continuing the vehicle theme, there is no real standard prescribing which of the control levers on the side of the steering wheel performs what function, even within a single manufacturer. When a driver moves from one vehicle to another, even if this happens regularly, it is all too easy to flash the headlights when trying to wash the windscreen or to indicate a turn when wishing to turn on the wiper blades.

Besides ergonomics, there are issues such as ease of use that contribute to the security risks that an enterprise may face in the Human Factors DI. For example, an enterprise may invest in robust technology to secure information, such as intrusion protection systems (IPSs), firewalls, data loss prevention (DLP) solutions and event correlators. While many of these devices are preconfigured with standard policies, they require customisation based on enterprise risk and network design. Mistakes in configuration may cause the machines to behave in unexpected ways, resulting in unforeseen security incidents; likewise, it is important that operational security personnel be trained in monitoring these devices so that when an incident occurs, it is noticed as soon as possible. In many instances, the initial security setup of an out-of-the-box technology solution is not what it should be, due to the fact that the initial configuration is considered the ‘bare minimum’, to accommodate as many customers as possible. Similarly, introducing new rules and customising a security solution may not be intuitive.

## 2. BUSINESS MODEL FOR INFORMATION SECURITY

The technologies implemented by the security organisation must also consider user acceptance. If the technologies designed to protect information assets begin to stifle productivity or otherwise interrupt daily operations, they cannot be considered efficient or effective. Hence, it is imperative that user acceptance be considered when implementing controls. The Human Factors DI is one of the motivators that shape user behaviour, whereas the other is the Culture DI. Both influences should be taken into account.

It is a known fact that humans can and do go around security controls. Many enterprises have implemented the latest and greatest technologies only to have employees work around the controls. While the latest and greatest technology is fantastic, on its own it may create a new risk to the enterprise: a false sense of security. An example of a false sense of security is the current controls used at airports. Is the traveling public really more secure when flying because of the often intrusive security procedures required between check-in and gate, or are these security procedures merely a 'show', with no real value?<sup>37</sup>

All of the security in place since the 11 September 2001 terrorist attacks on various US targets has failed to identify at least two high-profile known terrorist attempts on planes. In both of these situations, the alleged terrorist knew what security controls were in place and avoided them by either hiding materials in unchecked areas or using non-liquid materials for explosives. This phenomenon is partially due the Emergence DI and Human Factors DI. The perpetrators reversed the linear (and reactive) thinking of security management by simply exploiting a combination of factors and security loopholes that had not been considered before. They studied the security measures in place and then attempted a security breach in what they regarded as a weak link in the chain. In terms of human factors in security, this highlights how individuals will systemically out-think the existing security arrangements.

As a result, reactive, additional controls were enacted that may make people feel safe, but may not actually mitigate the risk of terrorists smuggling weapons onto a plane. In fact, the controls forced emergence. After the initial shoe-bombing incident, many airports forced passengers to remove their shoes and not carry liquids on a plane. In response, terrorists plans continue to evolve and exploit different areas in the perimeter where security is not as tight, while ordinary people suffer from frozen feet while standing in line. In contrast to the systemic thinking that potential terrorists apply, reactive security at airports does not factor in holistic security thoughts: adding more controls and making flying generally more cumbersome does not add to the factual level of security.

As mentioned before, information technology can provide the answers, but the answers cannot replace asking security questions. When people simply rely on the technology without understanding it, even the more obvious security weaknesses are often overlooked. This applies to all levels of the organisation:

- Executives place excessive reliance on information technology and other mechanistic solutions to provide the necessary security infrastructure.
- Managers rely on the existence of controls based on the security policy to ensure that there are no weaknesses.
- Staff are comfortable that they do not represent a security weakness because this is someone else's responsibility, and following procedures to the letter is a reasonable safeguard.

The potential issues which must be addressed by this DI therefore include, but are not limited to:

- Failure to understand not just the security requirements, but the reason for them
- Failure to appreciate the concepts of business risk and the possible impact of security weaknesses
- Failure to be aware of, and implement, the available system controls that support information security
- Human error in the form of poor memory or a simple lack of attention to detail
- External human factors such as bribery, corruption and social problems, which can influence the level of security awareness and adherence to controls
- Natural human tendencies whereby people misuse computer facilities for their own purposes

Naturally, this relates not only to the Human Factors DI, but also to the overall model. This fits in with the holistic nature of BMIS and the interdependencies amongst all elements and DIs within the model.

The impact of the Human Factors DI on the People element and the effect of the element on the DI are, therefore, easily understood but hard to address; however, this linkage may well be the most critical for the security management system to address what is often the weakest part.

Some individuals have a natural aversion to the use of any technology (not just IT), and this has a material, and probably detrimental, effect on the Technology element. People may be confused or annoyed by technical controls that cause delay in productivity. Typically, there are multiple reasons why people may not want to embrace technical security controls. Issues such as age, technical experience and tolerance for ambiguity all factor into their effectiveness.

---

<sup>37</sup> Schneier, B.; *Schneier on Security*, Wiley Publishing, USA, 2008

# THE BUSINESS MODEL FOR INFORMATION SECURITY

Age and education alone, however, do not indicate correct usage of IT. The information security management system must also address the potential lack of understanding by ensuring that 'mistakes' cannot happen. As an example, a major bank suffered a series of serious and damaging computer virus 'infections' to the corporate network. Upon investigating the incident, forensic analysts learned that:

- Users within branches had found that they could speed up network response times by switching off the desktop antivirus software.
- Users had a poor understanding of not only the nature of a virus attack, but also escalation and reporting procedures.

The second issue was one of poor training and awareness, but the first should have been prevented by the IT department that set up the desktop configuration in such a way that users could switch off the antivirus software. This was a simple case, but it is so often the simple matter, easily overlooked when creating the security infrastructure, that can lead to the greatest weaknesses.

The Human Factors DI also influences the Technology element by requiring the installation of a number of technical solutions to intrinsically 'human' problems. These include, but are not limited to:

- Antivirus and other 'malware' software
- Firewalls to restrict Internet traffic
- Filtering software to prevent Internet misuse and identify attempts
- Network-based intrusion detection systems (IDSs) to identify inappropriate and potentially dangerous user access

In conclusion, addressing the issues of the Human Factors DI and its relationship with the People and Technology elements requires careful attention to detail; implementation and enforcement of all available system-based controls and restrictions; establishment of management or 'peer review' controls, as necessary; and, above all, establishment of an ongoing process of effective security awareness across the organisation.

Areas of interest for security practitioners include:

- Communication
- Job task analyses and usability analyses, including functional requirements and resource allocation
- Job descriptions and functions, job-related procedures and utilisation of these procedures
- Knowledge, skills and abilities
- Control and display design
- Stress
- Visualisation of data
- Individual differences
- Aging, accessibility
- Safety
- Human error

All of the areas listed previously should be considered and, where necessary, addressed to ensure that the effect of human factors on information security is beneficial and not counterproductive. If the only technology available to people is a hammer, how many security issues resemble a nail? And how many 'solutions' exist to hit it?



### 3. USING BMIS

While the model integrates all components and activities within a security programme, practical use should follow a number of phases. This phased approach ensures that the existing security measures and solutions are fully adopted into BMIS and existing investments are protected. Using BMIS is not about reinventing the wheel—whatever is in place within an organisation is a positive that should be recognised and used accordingly. Changes to the security programme that are a direct consequence of using BMIS are usually self-explanatory if the phases are implemented in a step-by-step manner.

At this stage, BMIS is a new concept that has not yet achieved wide recognition. However, ISACA is planning and conducting real-life case studies that will be published in due course to enable informed decisions about using BMIS in practical security programmes. The following section, therefore, addresses the generic phases that are needed to:

- Fully integrate the existing security programme.
- Analyse and internalise the detailed security measures and solutions in place.
- Align current standards, regulations and frameworks to BMIS.
- Clearly identify strengths and weaknesses in existing security.
- Use the dynamic security system that BMIS introduces.
- Manage emergence within the organisation to maximise security improvements.

The first assumption in systems thinking is that changes to one end of the system will inevitably cause changes in other parts. When using BMIS, the traditional approach of doing one thing after another will work only when the dependencies amongst these activities are well understood. A look at the model makes it evident that changes within an element will also influence the DIs and, subsequently, the other elements; however, this should be considered an advantage: In many instances, changes to an element that is not directly in focus can bring about the desired changes in other parts of the security programme. Experienced security managers know this—just think of the sudden changes in human behaviour that come with a new chief executive officer (CEO) who happens to be interested in security as a theme. Word goes around that people should be careful about what they do, and there is a subtle and seemingly sudden modification to the culture of the firm. While the change of senior personnel has initially changed organisational culture as a whole, the systemic view further shows how this culture change is reflected in all elements and DIs of the model.

---

**When using BMIS, the traditional approach of doing one thing after another will work only when the dependencies amongst these activities are well understood.**

---

In practice, using BMIS will lead to a lot of change. Initially, the static elements of the security programme are brought into the model. This includes concepts and policies as well as technology. Standards that are in use or frameworks in IT form part of this exercise of populating BMIS with what already exists. Step by step, a picture will form that clearly highlights strong and weak areas in terms of elements and DIs. As an example, the Organisation element of security may be a strong point, but the People element and Human Factors DI may be weak points in the overall picture. At this point, the model shows its true value: Security weaknesses may be observed in any part of the enterprise, but the root cause may be in an entirely different area. The systemic work on elements and DIs helps discover these cause-and-effect relationships, and actions can be defined to improve on weaknesses.

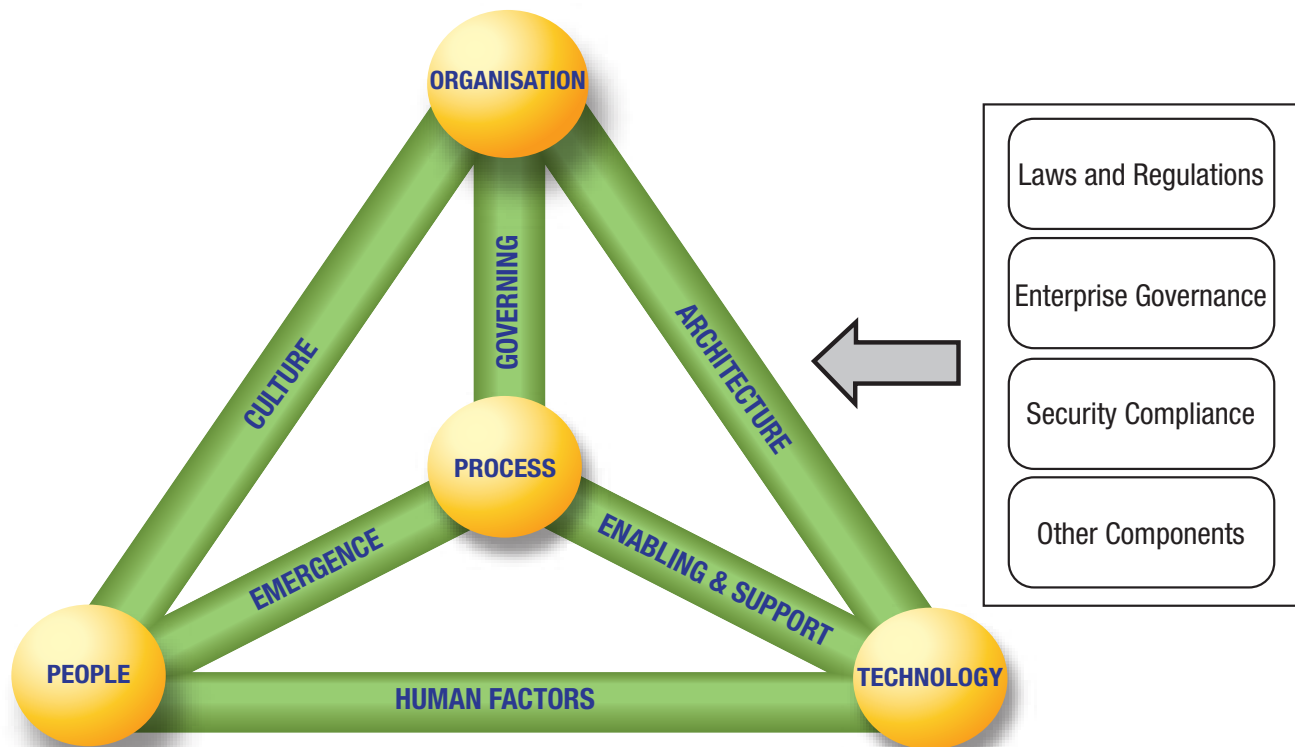
Subsequently, any changes in the business can be fed forward into BMIS and translated into adaptive security changes. The model will in turn visualise the feedback that occurs inside the overall system and clearly show what a business change means and what needs to be done to internalise it into the security programme. Likewise, emerging behaviour patterns, technology and trends in governance can be fed into the model, which will address them inside the security programme.

#### **Taking Stock: Analysing the Existing Security Programme**

In most enterprises, some form of security programme is already in place. This may be in the shape of a set of policies and rules, or a collection of technical solutions. The security programme is subject to the overarching direction provided by enterprise governance and its subsidiary areas, namely governance of IT and—in some cases—detailed security governance provisions. The security programme implements a layer below the overall governance framework. Although enterprise governance and related items are external forces, they clearly influence BMIS and how it is used in accordance with the accepted rules that have been set down for the enterprise. In addition, it is likely that at least one person is responsible (to an extent) for managing and maintaining security. However, whatever exists in terms of information security may well be heterogeneous and fragmented, sometimes with known gaps. As an initial step towards implementing BMIS, management should take stock and look at the existing programme and solutions, as shown in **figure 20**. This exercise can be less rigid than a formal security audit since BMIS in its subsequent phases will revisit the ‘taking stock’ phase at regular intervals.

# THE BUSINESS MODEL FOR INFORMATION SECURITY

Figure 20—Taking Stock: Analysing the Existing Security Programme



The following paragraphs give a brief outline of analysing the existing security programme. There are many other ways of performing this analysis, and any of them may be used. To maximise efficiency, security managers should also look to internal audit reports, external audit reports, certification reports and other sources of information that may be relevant to security. In large enterprises it may be advisable to enlist the help of external experts to ensure that there is a clear and unambiguous result of the analysis phase.

## **Laws and Regulations**

As a first step, the business should be analysed in terms of geographic location, customer and vendor relationships, and the supply chain in general:

- Where is business conducted? What are the relevant countries?
- Are there any high-risk countries in terms of security-related laws and regulations?
- Are there any 'outliers', e.g., customers or vendors that fall outside the main countries where business is done?

Once the relevant countries, regions and other distinct business drivers have been identified, the applicable laws and regulations can be mapped to the security programme, and later to BMIS. As an example, an enterprise doing business in the United States and Europe will find both sets of applicable data privacy and data protection laws: the US follows one approach, whereas most European countries favour a more stringent privacy perspective. The corporate security programme needs to take into account both approaches to provide assurance in terms of the law. This is not done by information security alone—the programme will normally rely on existing organisational strategy and design that defines and regulates privacy at the enterprise level. Admittedly, it may be a daunting task to identify and understand laws and regulations for any number of countries. However, there are commonalities in terms of information security that will enable management to define minimum standards.

Any applicable laws and regulations will usually map to the Organisation element of the model. They are managed and monitored as part of the organisational structure in security and any changes will be triggered from within the organisational structure. In this sense, security-relevant laws and regulations are no different from any other mandatory requirements in other parts of the business. The subsequent interpretation of laws and regulations resides in the Governing DI, as the enterprise gradually ensures that any and all internal rules are aligned with external requirements.

### **Enterprise Governance**

In some jurisdictions, laws and regulations are complemented by rules or codices of enterprise governance. The latter may have an impact on the security programme if an enterprise decides to adhere to them, or if adherence to enterprise governance is required for other reasons (listings, ratings, etc.). From the BMIS perspective, it is the enterprise itself that accepts and adopts external non-binding rules and makes them part of the organisation strategy. The security programme should take the non-binding rules and laws and regulations on board as part of adhering to overall enterprise governance as it has been defined at the strategic level.

In terms of identifying elements of the governance of IT and security governance, the simplest approach is to use the COBIT framework as a common language for expressing governance objectives and requirements. As a result, security management should address:

- Governance rules or guidelines adopted by the enterprise
- IT-relevant and security-relevant parts of these rules or guidelines
- Mapping of security-relevant governance items to the COBIT framework

Similarly to laws and regulations, enterprise governance maps to the Organisation element of BMIS, and it is implemented at the lower levels through the Governing DI.

### **Security Compliance**

In addition to specific security requirements in legislation and regulation, enterprises need to ensure a general level of security compliance. This is a direct result of other business requirements—for instance, accounting and finance and external audit requirements. As an example, the US Sarbanes-Oxley Act of 2002 requires an internal control system over financial reporting.<sup>38</sup> Most enterprises rely heavily on IT to implement and conduct their financial reporting process. It follows that IT controls and compliance are critical factors in general compliance. There are many other compliance requirements that may vary between enterprises and industry sectors, for instance:

- Financial audit, accounting and controlling
- Risk management, specifically operational risk
- Data archiving and retrieval

Compliance requirements normally map to two elements of BMIS: Organisation and Technology. In some cases, a mapping to the People element may be needed if personal behaviour is a compliance theme. The high-level recognition of compliance requirements is part of the Governing DI, in line with laws, regulations and enterprise governance. Lower levels of compliance requirements, such as in data management, are more likely to belong to the Architecture DI. Compliance required at a personal level should be reflected in the Culture DI, such as when people are expected to make a personal commitment to a code of ethics or other document that mandates personal responsibility and adherence to rules.

### **Other Components of the Security Programme**

The stock-taking exercise should be concluded by identifying and listing any other parts of the existing security programme that do not fall under the previous headings. In many enterprises there are links between information security and general (physical) security that should be considered for inclusion. Likewise, the use of external security services—such as certification auditors or electronic surveillance—should be analysed to ensure full knowledge and a detailed view of the existing security programme. Some of these components may include:

- Corporate security policies and standards
- Facilities management and information and communication technologies (ICT) continuity management programmes
- Business continuity management programmes
- Health and safety policies and procedures
- Certification requirements, such as the ISO 27000 series or the new service auditor standard (SSAE 16/ISAE 3402)
- ‘Bridge’ concepts and related programmes, such as monitoring programmes, external security services and outsourcing arrangements

Depending on the security component to be integrated, the mappings to BMIS will be to all elements and all DIs. Each component or service should be examined in detail and then provisionally mapped to an element and/or a DI.

<sup>38</sup> For a detailed view on the IT-related requirements and the mapping to COBIT, see the ISACA publication *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting*, 2<sup>nd</sup> Edition, USA, 2006.

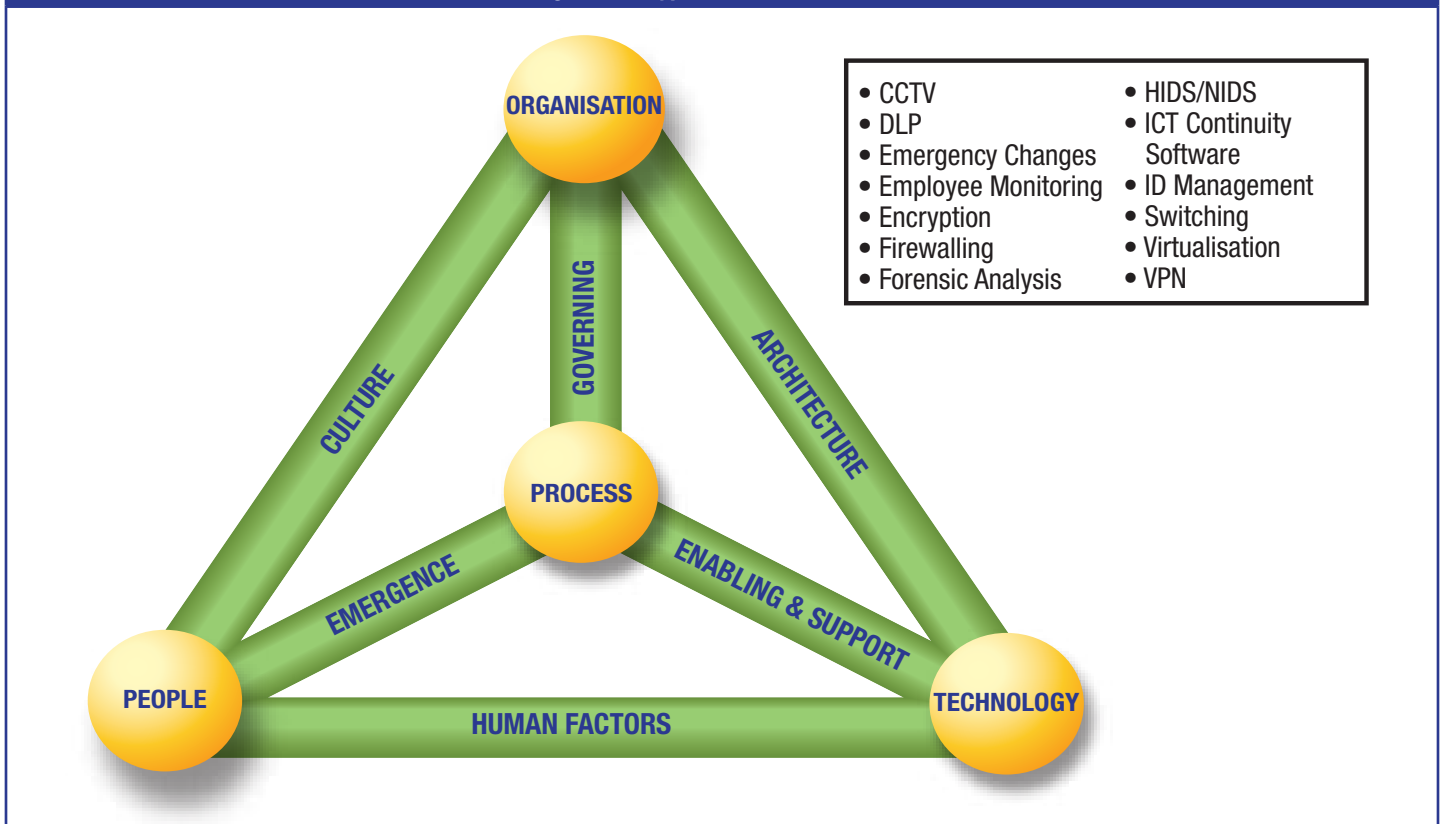
# THE BUSINESS MODEL FOR INFORMATION SECURITY

## Populating BMIS: Existing Security Measures and Solutions

### Gathering Information

While the overall security governance and management framework is an umbrella that covers all aspects of the Technology, Process, People and Organisation elements, there are many technical or other solutions and practical steps to implement, enforce and monitor security throughout the enterprise. For BMIS to be effective, these need to be taken on board and properly integrated, as shown in **figure 21**. The model in this context can be seen as a superstructure that is populated, step by step, with what is already there. Naturally, there will be stronger and weaker areas, but it is important to identify all technical and process solutions first.

Figure 21—Typical Solutions and Tools



The individual security solutions and measures taken are usually documented as part of the overall framework that the enterprise has decided to use, such as ISO 27001. For each area it will be easy to identify any number of technical or managerial detailed solutions that address specific security concerns. As an example, the enterprise perimeter might be protected by both firewalls (and demilitarised zones [DMZs]) and intrusion detection systems (IDSs—host-based [HIDS] or network-based [NIDS]). In terms of detailed security processes, the security manager may have introduced continuous monitoring or a forensic sampling of logs.

When using BMIS, security managers should gradually work their way through the various components of the information security management system and collect information on the resulting operational solutions, tools and processes. This list does not have to be exhaustive since the dynamic nature of BMIS allows subsequent changes and additions.

### Integrating Individual Solutions

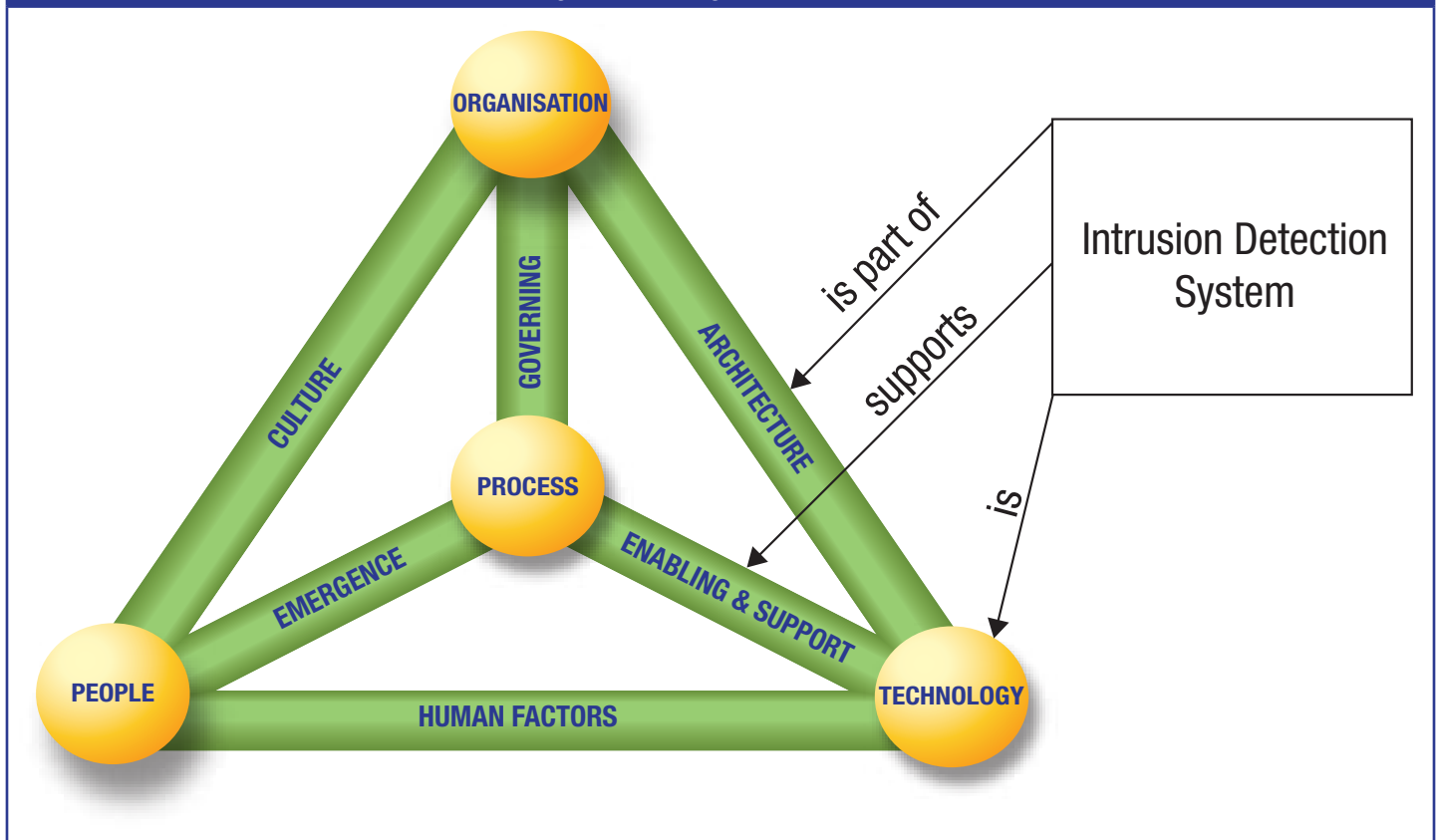
Once the majority of security measures and solutions have been identified, integrating them into BMIS is straightforward. They are matched against all elements and DIs to identify the relevant links (shown later in **figure 25**). The three points to address are simply:

- What is the solution (technology, organisational step, process, people-based)?
- What does the solution do and what security risks does it address?
- What does the solution support?

As an example, an intrusion detection system ‘is’ technology (more specifically, a combination of hardware and software). It should be managed as such and therefore clearly lives in the Technology element of BMIS, as shown in **figure 22**. Intrusion detection is a process (whether software-based or not) and ‘does’ just that—alerts management to any attempted intrusion or breach from outside of the firm. In this sense the intrusion detection system as a technical solution lives in the Enabling and Support DI, and in the

Architecture DI. Intrusion detection enables and supports the process of defending the perimeter, but it is only a part of that process. It further provides an important element that supports the security organisation (and managers tasked to monitor any security breaches), but it is only a part of the overall architecture. In combining all of these thoughts, the intrusion detection solution is firmly placed in the Technology element and in the two DIs linking Technology to other BMIS elements.

Figure 22—Linking a Solution to BMIS



For a typical technology solution to a specific security concern, it is less likely that the Human Factors DI (the behaviour of people and their interaction with technology) will play a role since intrusion detection is mostly handled by IT experts and less so by users. However, in a small company or organisation, it may be possible to draw another line from intrusion detection to the Human Factors DI, such as cases in which users install IDS software and configure it themselves. Even in an illustrative example like **figure 22**, the IDS turns out to be a potential source of systemic failure: where users are present, the Emergence DI may influence the process of intrusion detection, thus leading to changes in the process itself or in the way the software is used. This, in turn, might have been caused by the Culture DI that has influenced people to change their behaviour and subsequently cause emergent new behaviour.

For other, less technology-oriented security solutions, BMIS integration may require more links. For example, an innovative process for emergency change management may have significant security implications, but it is not entirely owned by security management. In these cases, BMIS once again allows a very simple integration by separating the security-relevant parts of emergency change management (see **figure 23**).

The existing solutions, once integrated, will eventually form a pattern that is mirrored in the elements and DIs, as shown in **figure 23**. Each element will cover a number of solutions, as will each DI. As a convenient side effect, looking at each element/DI and how it is populated will almost immediately show any gaps that exist in the security solution landscape. However, the number of arrows in **figure 24** clearly indicates that gaps in one element or DI may be difficult to close directly. A subsequent section, Identifying Strengths and Weaknesses, outlines a pragmatic approach to identifying and closing security gaps that are visible after populating BMIS.

After populating the model, it is useful to set up mappings of existing security solutions in tabular format, as shown in **figure 24**. The tables are an important tool for later assigning responsibility for tasks and actions that result from the BMIS view.

# THE BUSINESS MODEL FOR INFORMATION SECURITY

Figure 23—Integrating Other Solutions

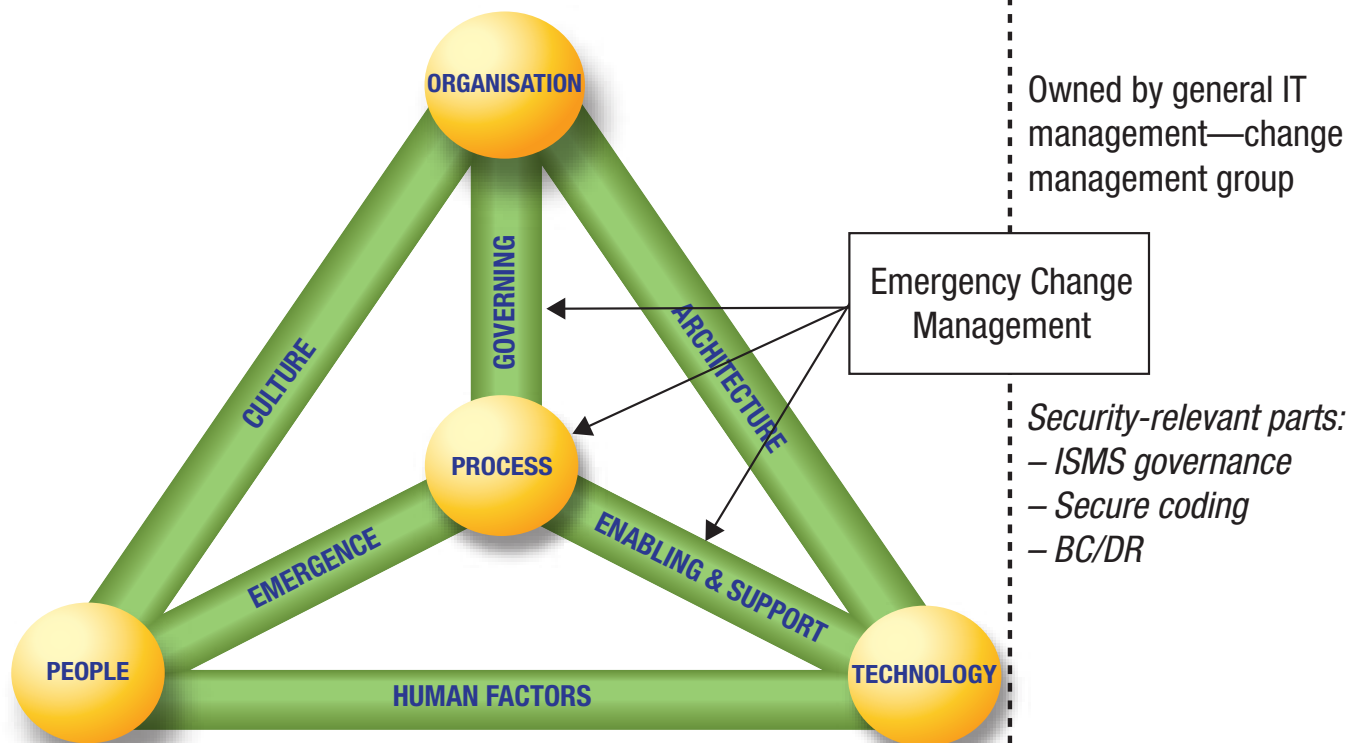


Figure 24—Elements and Security Solutions (Illustrative)

Element	Linked Security Solutions (*denotes partially owned)
Organisation	<ul style="list-style-type: none"> <li>• Corporate security policy*</li> <li>• Information security policy</li> <li>• Information security guidelines and standards</li> <li>• ISO 27001 certification cycle</li> </ul>
Technology	<ul style="list-style-type: none"> <li>• Identity and access management framework (including tools)</li> <li>• ERP security framework</li> <li>• Perimeter security (intrusion detection, DMZ)</li> <li>• Cloud/virtualisation (software as a service [SaaS], platform as a service [PaaS], infrastructure as a service [IaaS])</li> </ul>
Process	<ul style="list-style-type: none"> <li>• Security planning process (quarterly)</li> <li>• Security budgeting*</li> <li>• Information security monitoring process</li> <li>• Security enforcement process</li> </ul>
People	<ul style="list-style-type: none"> <li>• Training and awareness framework</li> <li>• Investigations*</li> <li>• Information security skills assessment</li> </ul>

In the course of using BMIS in practice, none of the initial solutions and security measures will be static. The systemic thinking behind BMIS requires frequent revisiting and updating the solutions and how they interact with the elements and the DIs. This should be regarded as an advantage: If BMIS thinking is applied to the annual planning, budgeting and programme management process, improvements will be more easily identified and shaped into information security projects. The link to the overall corporate objectives, as shown in **figure 25**—as a fundamental part of BMIS itself—further allows senior managers to clearly and concisely outline the risk return on any security solution or process.



Figure 25—Security Solutions Mapped to BMIS (Illustrative)

Solution	What It Is	What It Does	What It Supports
Encryption (mail)	Technology (software)	Protects confidentiality and integrity for flow data	Architecture (part of overall encryption and confidentiality)  Enabling and Support (supports mail and communications processes)  Culture (discourages the use of open e-mail channels for sensitive information)
Encryption (storage)	Technology (hardware and software)	Protects confidentiality and integrity for static data	Architecture (part of overall encryption and confidentiality)  Enabling and Support (supports storage/archival/infrastructure)
Incident management	Process	Controls incidents in IT	Organisation (governance, risk, compliance)  People (contain the personal impact of incidents)

In this sense, BMIS addresses business needs and requirements directly, based on strategic and tactical dispositions. The resulting business decisions are easily ‘translated’ into more hands-on activities and security measures to be designed and implemented by security managers.

### Example

In many enterprises, internal security breaches and ‘insider threats’ have been a significant security challenge for years. In actual fact, up to three-quarters of successful attacks are of an internal nature or started from within the enterprise. The problem is complex and it is systemic in nature:

- Insider attacks are comparatively rare, not unlike natural disasters or other low-frequency events.
- An ‘insider’ by definition is a legitimate user with either excessive access rights or in possession of a new way of attacking.

As a result, internal security threats are often seen as unpredictable and therefore unmanageable. This leads senior management to conclude that these attacks cannot be prevented, and no further action is taken. If, and where, an internal attack occurs, management is likely to be reactive, trying to contain the issue. At the same time, the focus of technological solutions shifts to external attacks—a more tangible and manageable item. In some organisations this may be accompanied by a culture of ‘trust’ that discourages talking about the possibility of internal attacks.

The solution in successful organisations covers many aspects of security. BMIS is an ideal tool to enable the integration of a comprehensive solution that addresses internal attacks on all fronts. As shown in the following paragraphs, the solution is entirely systemic and its success cannot be attributed to any single step—in practice, it takes a lot of work to reduce the number of internal attacks in any environment.

The first step in the solution is situated in the People element of the model. It is here that individuals act against the rules and against the interest of the enterprise. From a systemic point of view, their motivation may be profit or greed, general discontent with the workplace or management, lack of personal recognition, or any combination of these motivators. The following practical steps have been suggested to address these potential motivators:

- Improved human resource (HR) practices—Pre-employment screening, employee monitoring, employee assistance programmes
- Training and education programmes in compliance and responsible behaviour
- No exceptions for ‘star performers’, introduction and maintenance of clear limitations to what employees are permitted to do
- Enforcement of information security best practices, including identity and access management
- Open disclosure and legal action strategy—Publish and prosecute

To integrate the overall solution into the model, the steps need to be allocated to the elements and DIs on a ‘best fit’ basis.

## Example (cont.)

HR practices such as pre-employment screening reside in the Organisation element. While HR processes would be external to BMIS, their use in security-related recruitment is a given. Part of what needs to be done prior to and during employment of a person with wide-ranging access rights is in the Governing DI, as processes will be subject to restrictions coming from HR. In a business context, BMIS can further help identify any conspicuous patterns in employment—such as the inflow of fairly young individuals at low salaries, or the positioning of security-critical jobs in a no-promotion, not too highly regarded internal department. This will further help identify potential emergence issues, such as where employees have a sense of discontent that subsequently turns into a plan to attack the enterprise.

The training and education part of resolving the internal attack problem is often placed in the Organisation element and the Governing DI. Both training and other forms of education reinforce what the organisation expects of employees, but it is unlikely to be a deterrence to a determined attacker. For the great majority of employees, training and education reinforce what they already know; however, these steps clearly shape the Culture DI as well, in providing the ‘right message’ from the Organisation element to the People element.

In practice, enforcement of existing rules—without exceptions—is situated in the Culture DI. The Organisation element must communicate the appropriate message to ensure that within the People element, the ‘no exceptions’ rule is clearly understood. In systemic terms, enforcing the ‘no exceptions’ rule further strengthens the Governing DI and the Process element. It also influences the Emergence DI in preventing the emergence of practices that may be associated with individuals who consider themselves outside the normal set of rules.

Information security best practices need to be subdivided into their components parts. Integration into BMIS will likely be at the Organisation element level (through policies and standards), within the Technology element (applications supporting IAM) and within the Process element (processes linking to HR and general administration).

The final step towards full BMIS integration covers the disclosure and prosecution process, which is an important component of the overall reduction in internal attacks. In the first instance, this security measure is obviously situated within the Organisation element since it requires senior management decisions as well as rules outside BMIS. However, communicating and enforcing this course of action will have an immediate impact on both the Governing DI and the Culture DI.

In the previous example, the existing solution—as shown in the bulleted list—is integrated to BMIS, and any gaps will become visible once the problem of internal attacks is looked at systemically.

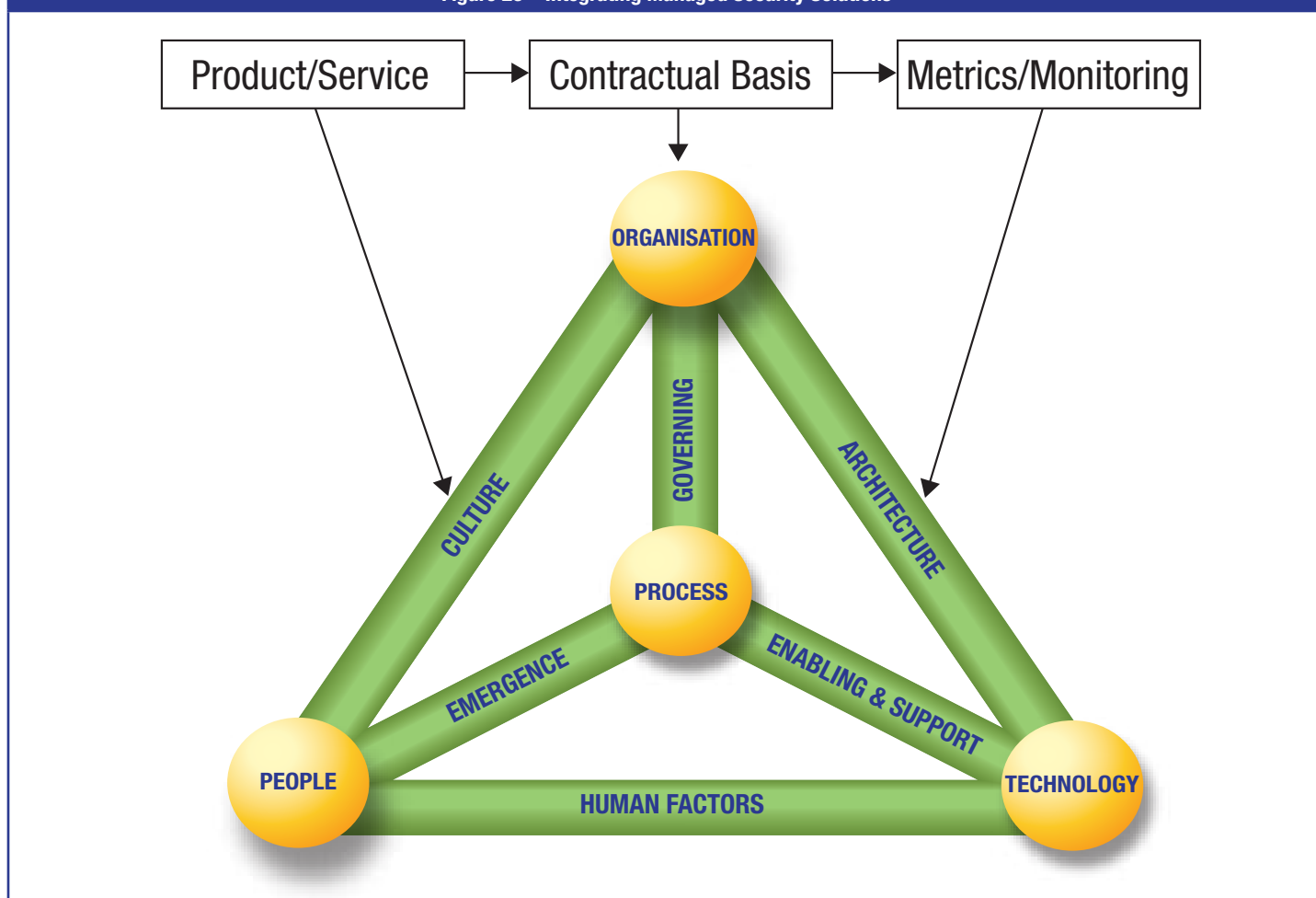
## Integrating Managed Solutions

In today’s corporate environment, many security solutions tend to be external and managed rather than internal. This creates many challenges and security managers need to rely on third-party service providers to a large extent. While most security models do not anticipate the outsourcing or third-party management of security-relevant products and services, integration into BMIS is quite simple. From a practical point of view, the product or service rarely changes just because it has been given to a third party. Vulnerability testing, for instance, is technically the same if done by an expert firm, as are security logging and analysis. The difference is often found in the contractual relationship, responsibility and accountability for critical security solutions. Managed solutions can therefore be conveniently subdivided into:

- **Process**—Parts of information security are PaaS.
- **Technology**—Security-related technology, hardware, software or technical services are bought in from an external provider (usually on a pay-per-use basis), such as SaaS/PaaS/IaaS.
- **People**—External resources are hired to do a security-related job.

From the BMIS perspective, all relationships with third parties and all managed products or services should be outcome-based. That is what the provider is paid for, and the result should be exactly what might be expected if the service were provided internally. It can therefore be integrated into the model just as any internal product or service, as shown in **figure 26**. The main difference is that delivery and quality are governed by a contract that states the relationship between two or more parties. In BMIS, the contract is placed in the Governing DI, where other (internal) governance instruments would be placed. In addition to having a contract, most enterprises apply metrics and measurements to better control contract fulfilment. Once more, the controls and measurement processes form part of the Governing DI since they clearly show how the Organisation (as an element) controls Process (as an element), even if these are bought in from an external source.

Figure 26—Integrating Managed Security Solutions



In terms of information security, managed solutions are thus very similar to internal solutions. In BMIS they are integrated just as any other solution, but an additional (contract and related controls) dimension exists.

### Aligning Standards and Frameworks to BMIS

Many enterprises are using a number of recognised standards and frameworks in information security. These are often seen as a subset of the wider range of general IT standards for governance, risk, compliance or IT operations. Adherence to a standard usually means that significant effort has been put into following the structure and requirements, particularly in technology. BMIS has been designed to have the inbuilt flexibility to adapt to most standards currently in use in information security. This includes, as a first layer, those standards that specifically address information security in the widest sense. The second layer of alignment covers general IT standards that have a direct or indirect impact on security. As a third layer of alignment, specific standards may have to be considered, depending on the industry sector and potential regulatory requirements. The following section outlines a practical approach to aligning BMIS with any existing standards an enterprise has already adopted.

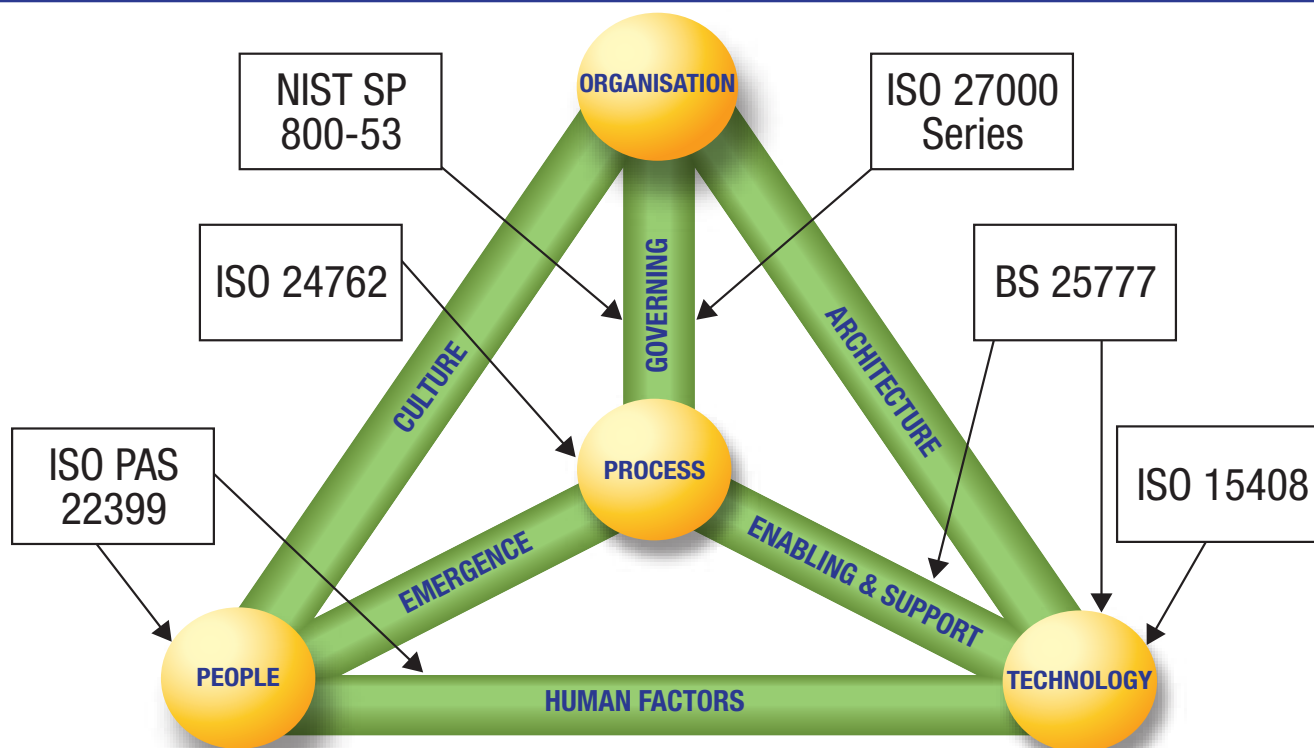
**BMIS has been designed to have the inbuilt flexibility to adapt to most standards currently in use in information security.**

#### Information Security Management

At the core of the standardisation within an enterprise, the information security standards used need to be aligned with BMIS. Policies and standards are positioned in the Governing DI of the model since they influence both the Organisation and Process elements. The model itself often needs further alignment in terms of the content of the standards, such as in physical security or access management. **Figure 27** shows how standards are aligned with the overall model as a first step, and **figure 28** illustrates the alignment of BMIS to individual chapters and content of the standards.

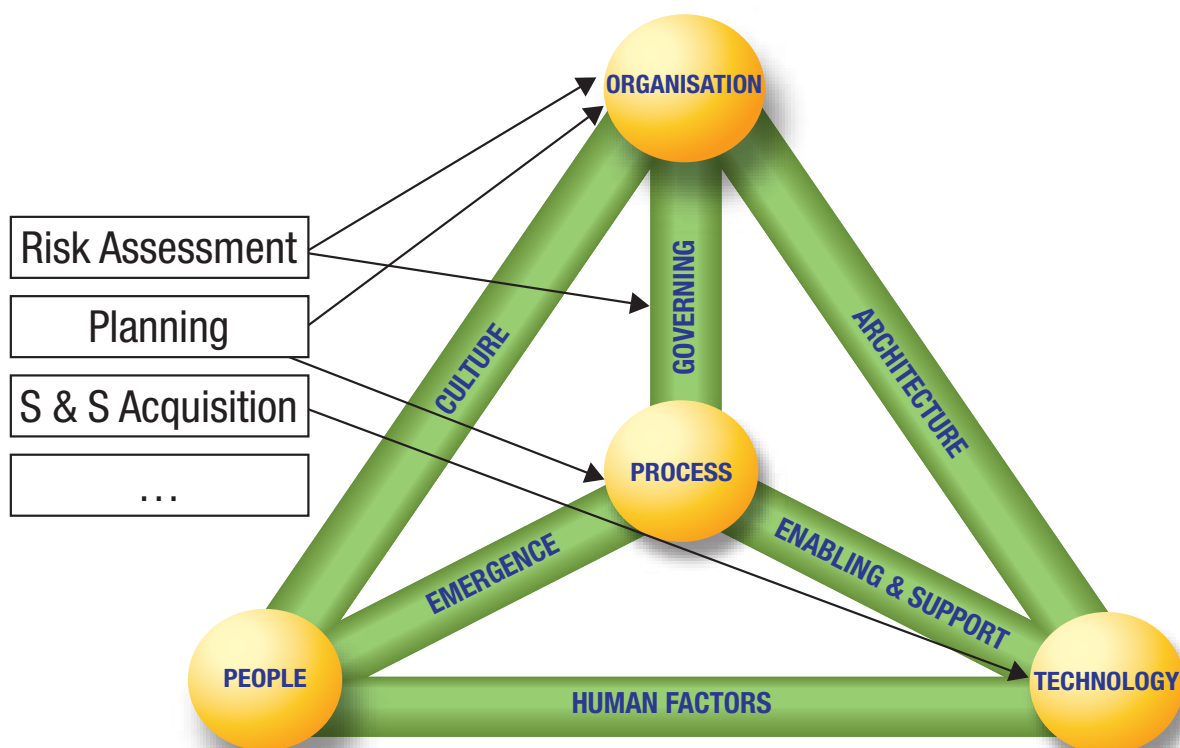
# THE BUSINESS MODEL FOR INFORMATION SECURITY

Figure 27—Common Security Standards and BMIS



Depending on which information security standards are used at the enterprise level, the alignment may have to be repeated at regular intervals, as when a standard is updated or extended by the issuing organisation. This may be the case where a series of standards feeds into one or two high-level norms, such as ISO 27000.

Figure 28—Contents of NIST SP 800-53 Aligned to BMIS (Illustrative Example Only)



For each standard, security managers should map the individual chapters or clauses to the elements and DIs within BMIS. In practice, this will lead to a number of relationships between the model and the detailed content of the information security standard, which will also help identify responsibilities and roles within the information security organisation. For instance, the person(s) responsible for risk assessment from a standards perspective would be assigned to parts of the Organisation element and the Governing DI.

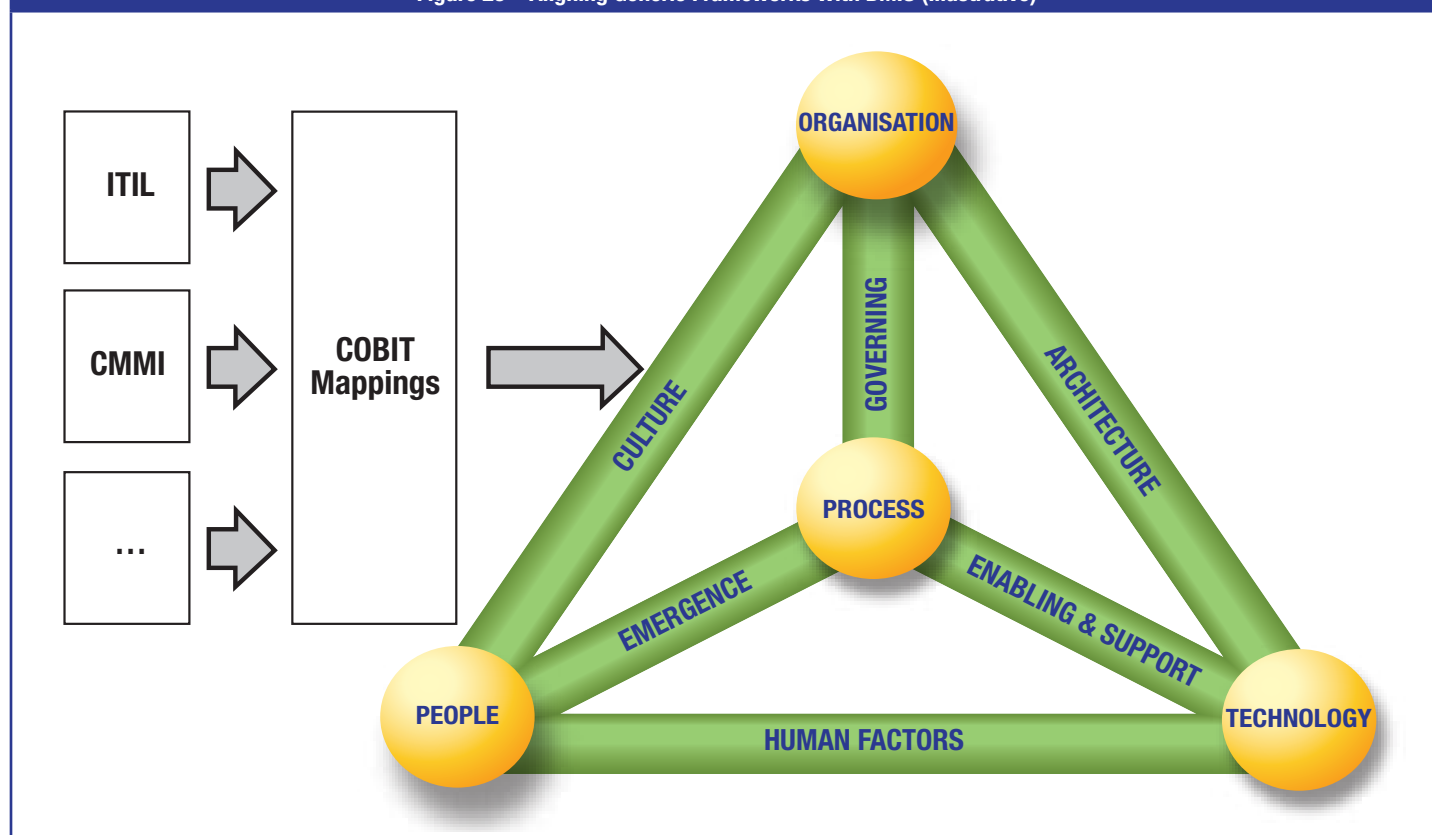
## General IT Management

In addition to specific information security standards, many enterprises have adopted and implemented more generic IT management guidance such as Information Technology Infrastructure Library (ITIL). While these standards are much broader than just security, they often contain important components that need to be considered when working on information security. BMIS should therefore align to these more generic standards and frameworks in a way that is similar to the specific standards (see the previous section).

Security managers should look to the COBIT framework, which will facilitate alignment between general IT management and BMIS, as a convenient tool. **Figure 29** illustrates how most recognised standards have been mapped to COBIT,<sup>39</sup> which can act as a hinge between the standards and the model.

**Security managers should look to the COBIT framework, which will facilitate alignment between general IT management and BMIS, as a convenient tool.**

Figure 29—Aligning Generic Frameworks With BMIS (Illustrative)



## BMIS Diagnostics: Identifying Strengths and Weaknesses

Once the information security solutions have been integrated with the model and the alignment to existing standards has been completed, the next step in using BMIS is a thorough analysis of strengths and weaknesses. In most enterprises some aspects of information security are well developed, whereas others may be less mature. While this tends to be known to security experts, the use of BMIS enables management to identify causes and effects. An example is a weakness found in a technical solution that should not be seen in isolation since the root cause may be an architectural flaw or even a policy issue. Similarly, a strong point in technology may be the result of an organisational action or simple emergence. To avoid working on the symptoms, BMIS can help in structuring the analysis of strengths and weaknesses.

<sup>39</sup> In its future versions, COBIT will naturally integrate BMIS to a large extent, making it even easier to align IT management standards.

# THE BUSINESS MODEL FOR INFORMATION SECURITY

## Situational Analysis

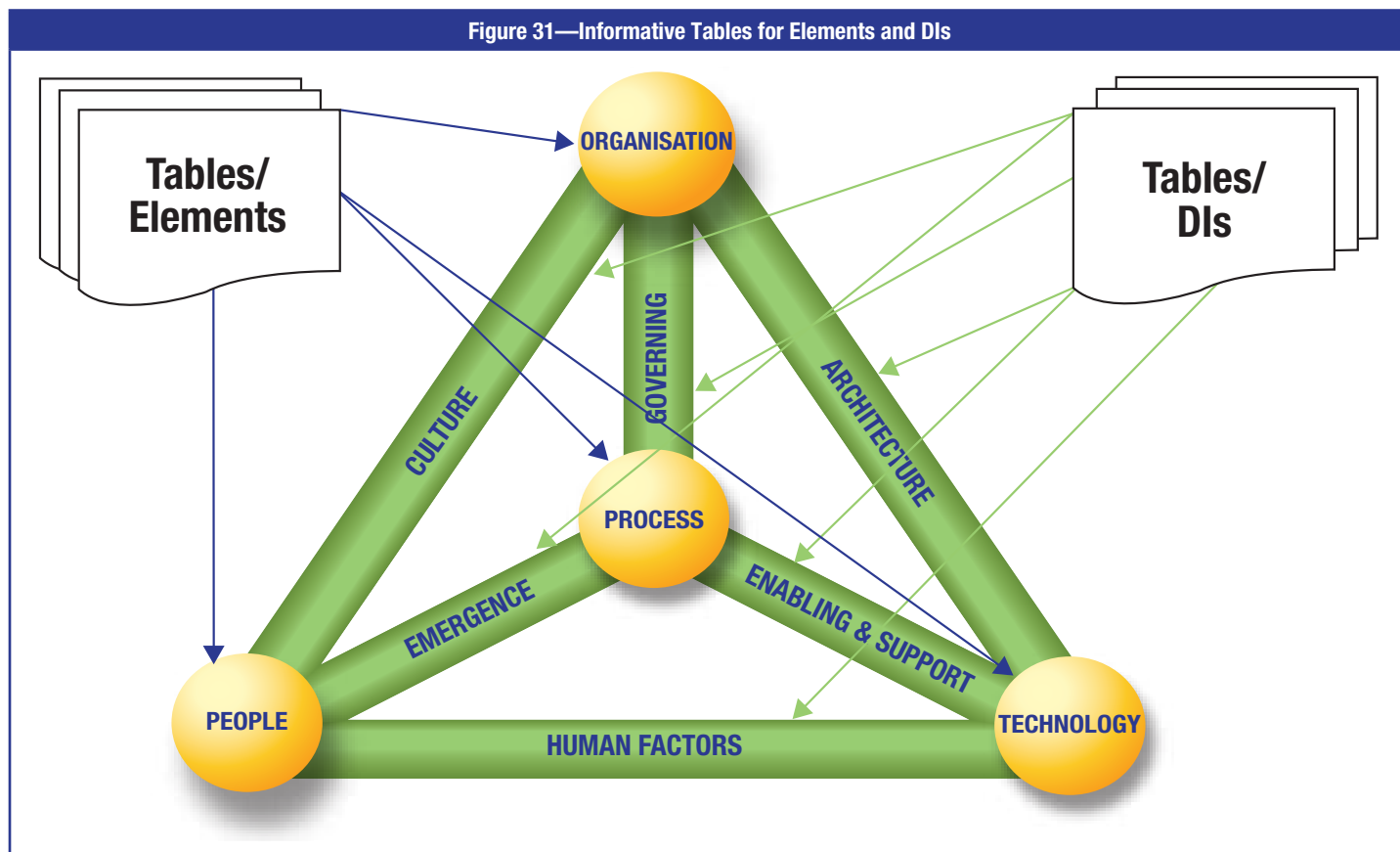
The first step in identifying strengths and weaknesses is a thorough analysis of the situation based on the fully populated and standardised BMIS. Given the systemic approach that is at the heart of the model, any element or DI is a good starting point. For each element, the model should contain the minimum information added previously:

- Existing policies, methods and controls
- Existing detailed solutions, tools and procedures
- Relevant parts of information security standards
- Relevant parts of general IT standards

The simplest way in which this information may be represented is a tabular format, as shown in **figure 30**. While such lists may be fairly long at first sight, they are easy to manage and update in subsequent cycles of BMIS activity.

Figure 30—Listing of Strengths and Weaknesses for the People Element (Illustrative)		
Item	Type	Strength/Weakness
ISO 27001: InfoSec Policy	Policy	Weakness—It exists, but is out of date.
ISO 27001: Employee Background Checks	Procedural	Weakness—It is non-existent.
ISO 27001: Employee Security Training	Procedural	Strength—It is well developed and held frequently.
ISO 27001: Employee Termination	Procedural	Strength—All criteria are met and there are no gaps in the exit process.

For each element and DI, this exercise will provide a picture of what has been done in security and the overall maturity level. While policies, standards and overarching controls are usually straightforward to identify and list, the requirements of information security standards and general IT standards are likely to be more comprehensive, but conveniently listed in the standards table of contents and structure. **Figure 31** shows the end result of this first step in the situational analysis. Once these tables have been consolidated, subsequent repeats of the situational analysis could expand on the information, perhaps in the form of balanced scorecards. However, the basic principle remains the same.





The second step in analysing the situation is to flip the tables in terms of each item. An example is the ISO 27001 requirement of having a security policy, which is likely to come up in several tables:

- Organisation element
- People element
- Culture DI

In many cases the same item—in this case, the policy—will receive a different rating, depending on the viewpoint. For instance, an information security policy might be seen as a strength in the Organisation element, but as a weakness in terms of the Culture DI. Similarly, employee security leaflets might be a strong point in the People element, but a weakness in the Organisation element. These differences will become even more visible in technical solutions or detailed procedures. In working through the tables, the result might look like **figure 32**.

Figure 32—Individual Item Mapping (Illustrative)			
Intrusion Detection System			
<i>Technology Element</i>	<i>Architecture</i>	<i>Enabling and Support</i>	<i>Human Factors</i>
Strength—It is a comprehensive technical solution.	Neutral—It is supported by the infrastructure.	Weakness—There are many false positives; it is slow; some real intrusions happen.	Neutral—Employees have no direct exposure to the tool.

The item shown in **figure 32** is a difficult one since it is obviously strong as a technology solution—or as the technology people see it—but less popular when viewed from the processes it is supposed to support. In practice, this is a phenomenon that security managers experience very often: an issue in information security is addressed from the technology point of view, but the reality within business processes is different. When reviewing BMIS tables in this way, a seasoned security practitioner will know immediately what is wrong with intrusion detection.

Once the situational analysis has been completed, BMIS will highlight these ‘symptoms’ of relative weaknesses or strengths and discrepancies in perception and evaluation. Likewise, any item that is unanimously evaluated as a strength will be clearly visible when comparing the tabular information. The systemic view ensures that each security solution or procedure is seen from all perspectives.

### Root-cause Analysis

Once the situational analysis has been completed, all strengths and weaknesses should be known for the complete set of elements and DIs. To maintain the strengths as they are and to address weaknesses, the root causes need to be identified. As indicated previously, in practice the real reasons for a security weakness that is seen in day-to-day business may be hidden or located in another part of the organisation. The systemic approach in BMIS is again helpful in providing a step-by-step guide to finding out more about the root causes. For any given security weakness (or strength), the following steps will reveal the full picture:

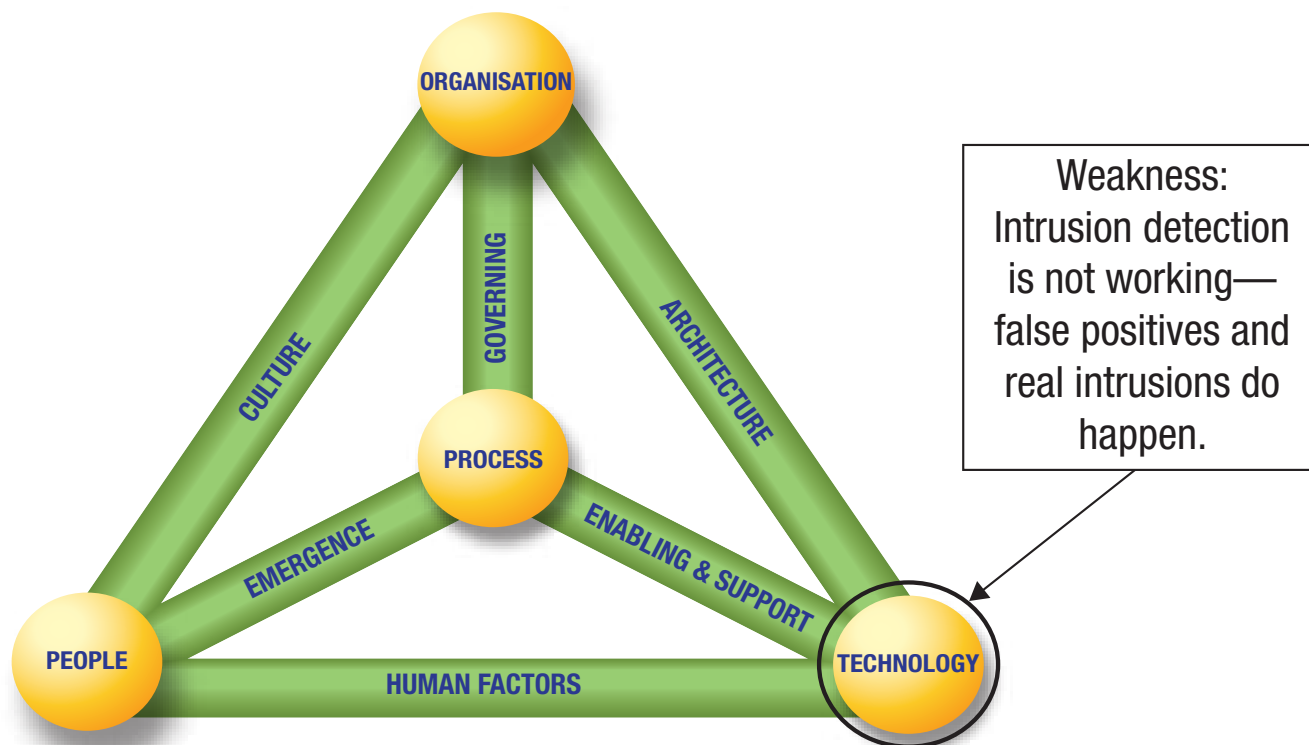
- Is this a trivial weakness (e.g., the tool is dysfunctional or needs bug fixing)?
- Is the root cause within the element(s) where the weakness is located?
- Is the root cause within the DIs pointing to other elements?
- Is the root cause in other elements and indirectly connected to the weakness?

An experienced security manager will perform all of these steps almost intuitively. In this way, many security problems are resolved very quickly. However, it is more convenient to be able to list issues and solutions within BMIS to ensure completeness and to clearly show the process of reaching a root cause after a number of logical steps. More often than not, experienced security practitioners get it right, but they find it difficult to explain how. In this sense, BMIS provides practical help in documenting the steps and the intuitive conclusions.

**Figure 33** illustrates a trivial weakness. The IDS appears to be less than effective since it causes false-positive alerts and, more seriously, fails to prevent real intrusions. The first idea is to check within the Technology element to determine whether the product used is causing difficulties, possibly through configuration errors or flawed installation. In this particular case, both root causes are quite likely since standardised IDS products have been around for some time and seem to be functioning fairly well in other practical situations. Fixing the configuration as a next step will either remediate the weakness (which should be instantly visible) or point to a more complex root cause.

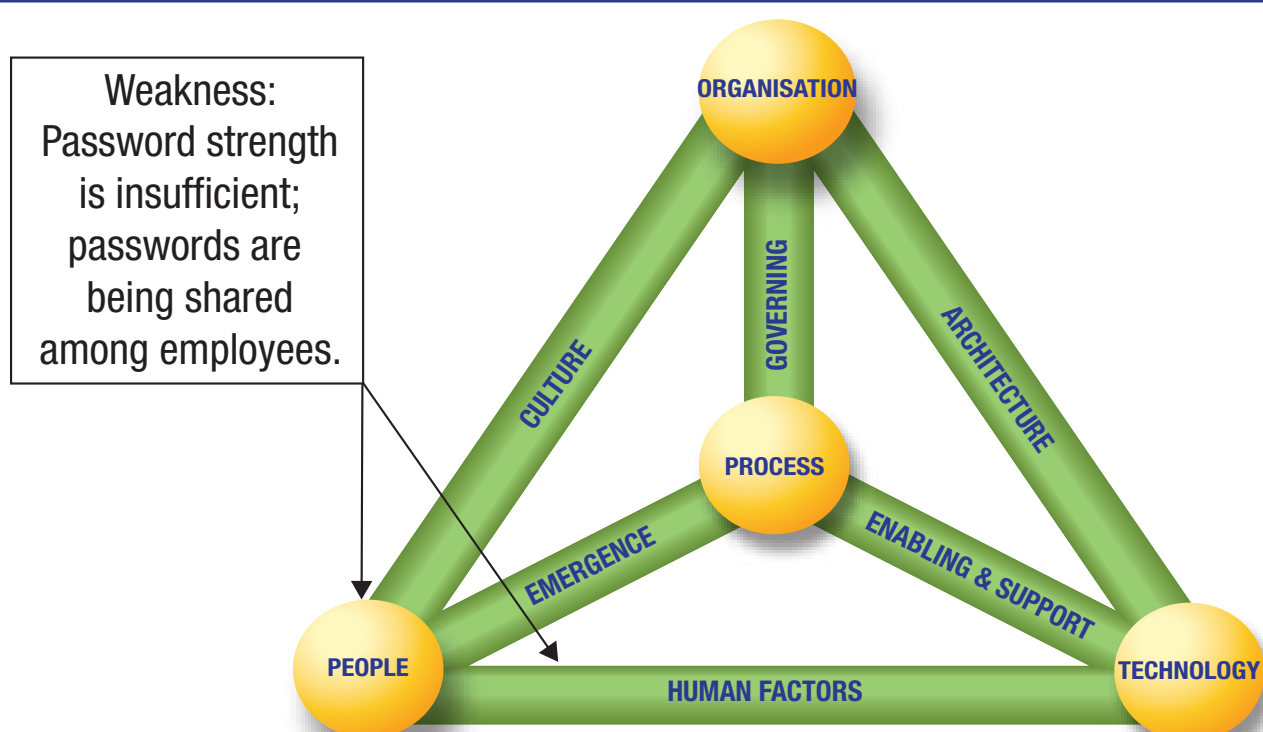
# THE BUSINESS MODEL FOR INFORMATION SECURITY

Figure 33—Root Cause: A Trivial Weakness



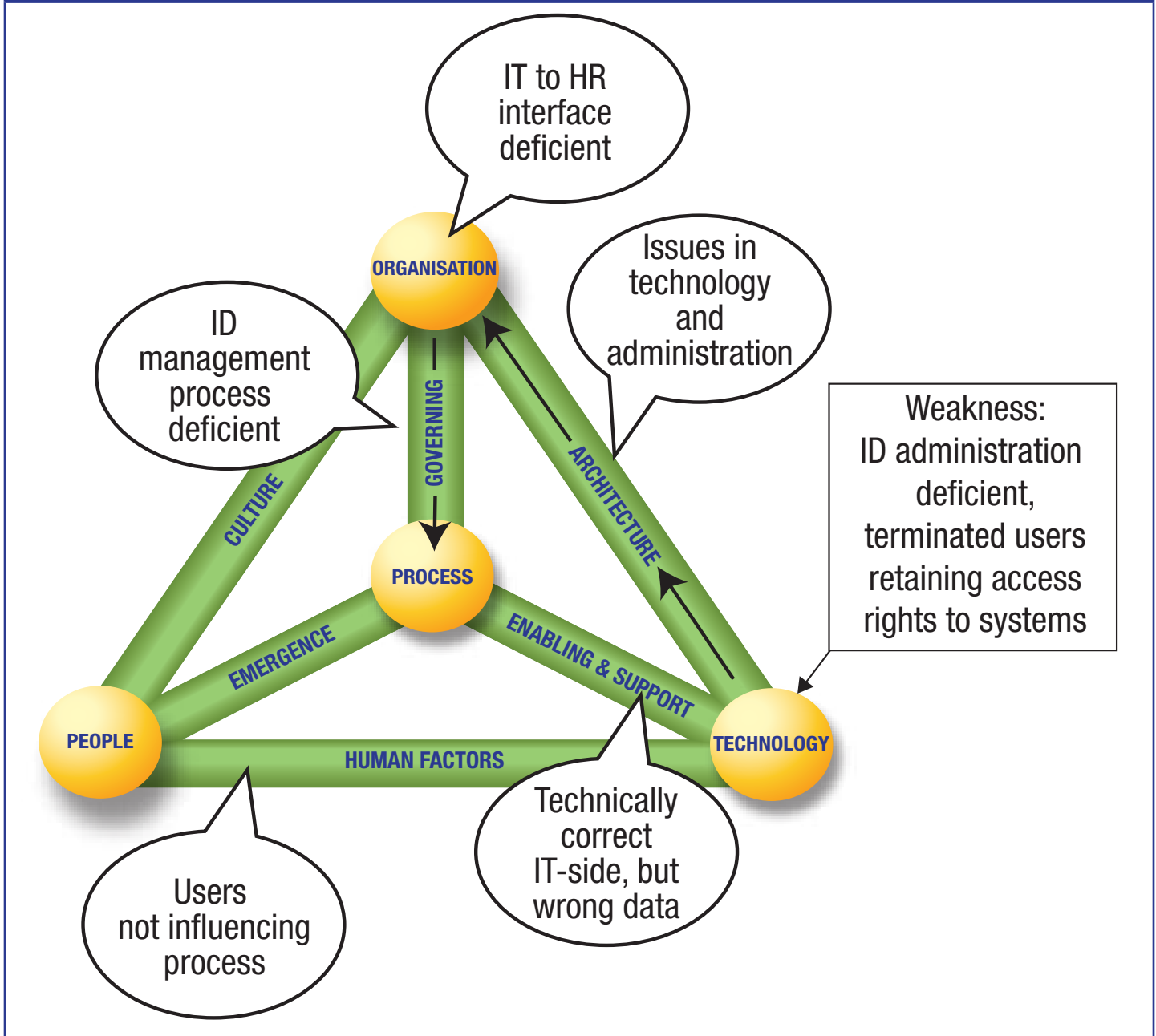
**Figure 34** shows how a weakness is first visible in the People element. In this case, the first symptom is that people are using weak passwords and password sharing has taken place. Both symptoms are definitely not appropriate in terms of information security, but the root cause is not a matter of individual preferences or unwilling employees. As a second step, the Culture DI can be left out of the picture since organisational structures and password policies usually exist. Practical password setting is, however, a matter of technology—how passwords are created, requested, stored, etc. It appears that users, for some reason, have difficulties with the way in which passwords are handled by the Technology element.

Figure 34—Root Cause: Weakness in Element and DI



For more complex weaknesses the systemic BMIS approach might look like **figure 35**. In this case, there is a well-known problem that is often seen in practice: While there are stringent technical controls in place for user access, in many instances, there are ‘phantom’ users who have long since been terminated. In this example, the IT process appears to be fine since all that is received into the ID management systems is duly processed. The problem is that the data on users are simply wrong. This could be due to any number of reasons, but it is clearly administrative and organisational in nature. The next logical step in a systemic view is, therefore, the Architecture DI, which highlights a disconnect between technology and the organisational aspect of ID management. This, in turn, leads to the question of how both processes (IT and HR) are governed and the subsequent impact on the problems observed. While the conclusion may be straightforward for the experienced security practitioner, stepping through BMIS clearly identifies the deficiencies and allows management to address them in a coherent manner.

Figure 35—Root Cause: Multiple Elements and DIs



This logical sequence should eventually fit with the previous tables (**figures 30 and 32**) that look at each information security solution and control from the point of view of the elements and the DIs. The root cause analysis part of working through BMIS should be a mirror image of the initial situational observations. For instance, where intrusion detection is recognised as a ‘trivial weakness’ in the previous example, this should fit in with the initial view on intrusion detection in **figure 32**. In actuality:

- Technologists see intrusion detection as a ‘comprehensive solution’, which it is from an off-the-shelf tool perspective.
- Architecture is neutral because, in theory, the tool should be working well.

# THE BUSINESS MODEL FOR INFORMATION SECURITY

- The Enabling and Support DI shows issues perceived by process owners in the operational IDS that are the only indicators (from a situational point of view) that something is amiss.
- The Human Factors DI is neutral because users have no way of knowing what is protecting them (or not).

This example clearly shows that the things observed in the situational analysis show only part of the picture. Root cause analysis reveals why the deficiency in the Enabling and Support DI is present and the underlying reasons for it. In a similar way, the example of ID management deficiencies can be worked through from the initial observations (situational) to the logical steps leading to a sensible conclusion.

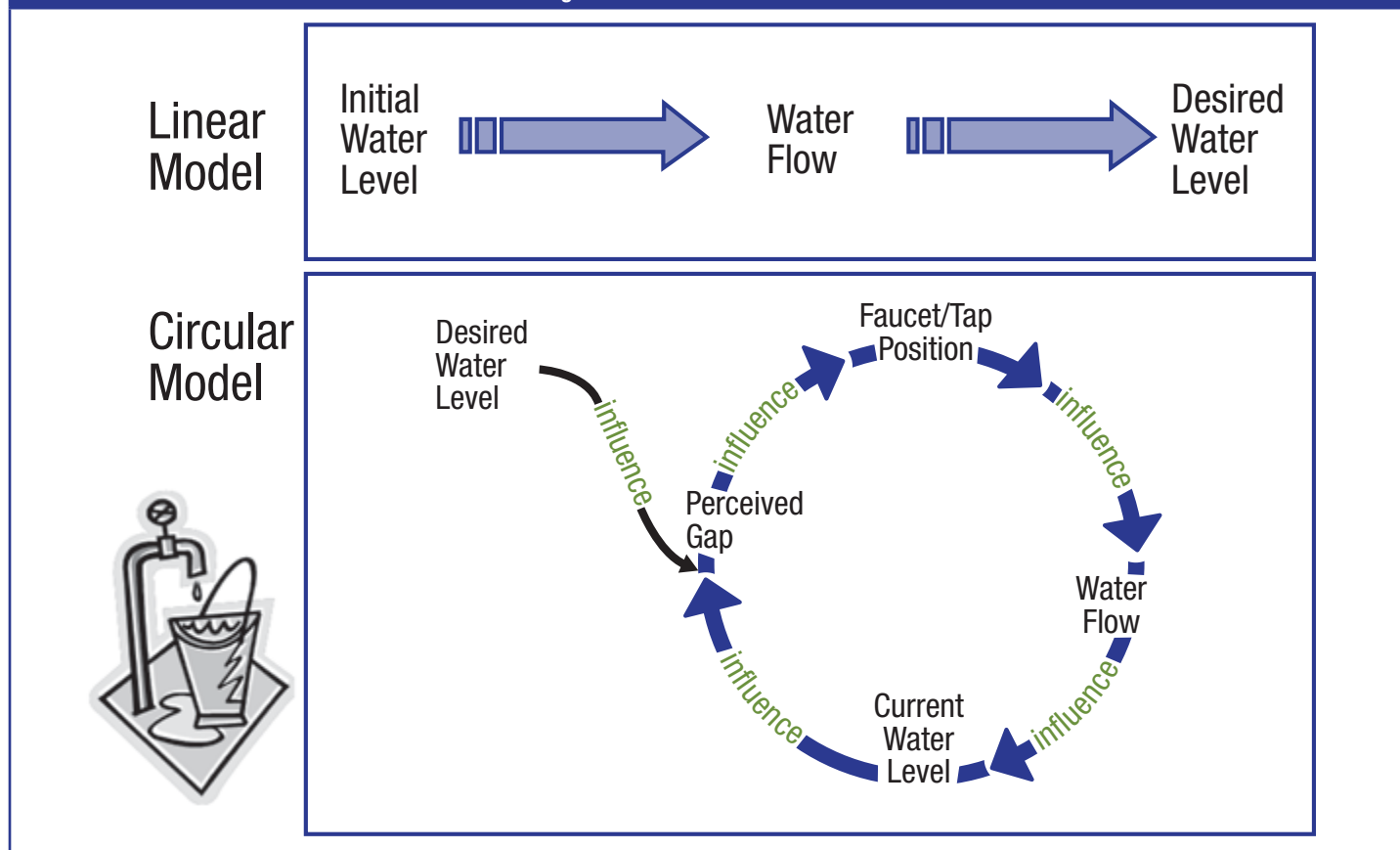
## Setting BMIS in Motion: Improvement Journey

If situational observations indicate one thing and root cause analysis leads to an entirely different perspective on strengths and weaknesses, the result could be a corporate information security environment in which it is difficult to remediate weaknesses or foster strengths that are evident. One of the most interesting questions is how the overall state of information security will change if action is taken or if targeted security investments are made. Success or failure of any security-related activity will be visible immediately, but it may be much harder to explain why certain things work and others do not. The simple example of password sharing as a security weakness demonstrates this: Are people sharing because the passwords are too complex? Or are they simply bogged down by red tape in their day-to-day business? The answers to these questions are important for security management since they will determine the course of action for remediation and improvement.

In any complex system, changing one thing will inevitably lead to more change in other parts of the system. To make this change predictable and controllable, traditional security processes and controls must be translated into subsystems of the overall information security management system. This first step in the improvement journey clearly shows how processes—subsystems—evolve over time and how they will react to changes introduced by security managers and practitioners. Breaking down the overall system into manageable components relates back to BMIS since the smaller subsystems are all within the elements and the DIs.

Security subsystems show immediately how they can be influenced by internal or external activity, and what the consequences will be if influence is exerted in one way or another. For the security manager, the BMIS approach highlights what an investment might achieve and what the desired (and sometimes inadvertent) outcomes might be. The model uses circular thinking rather than linear thinking, as illustrated in **figure 36**.

Figure 36—Linear vs. Circular View

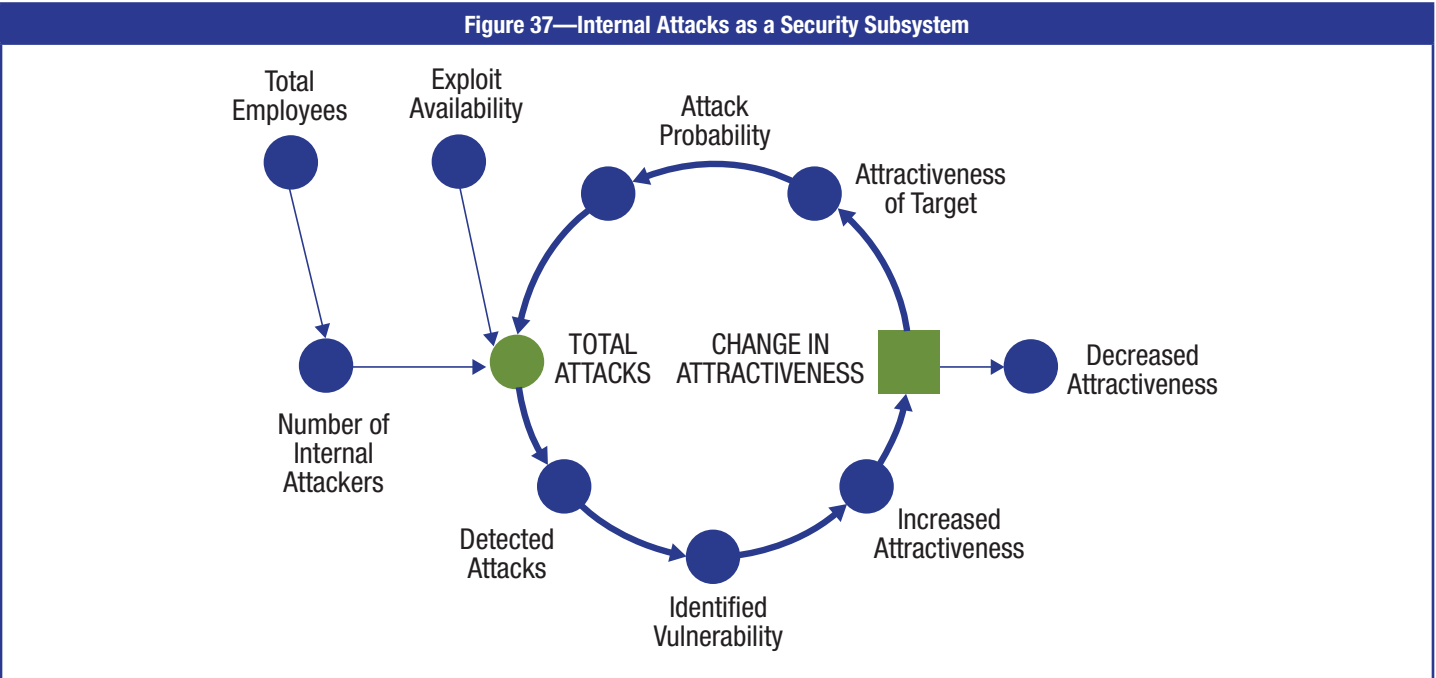


On the basis of circular security subsystems, improvement steps and actions can be targeted where they will be most effective. Individual actions and security measures are then embedded into the context of the overall system and how it behaves.

As a final step in starting the BMIS improvement journey, the model allows a clear view on how system dynamics lead to activities, behaviours and patterns that become more embedded over time, particularly in terms of the overall security level of the enterprise. One of the primary objectives in using BMIS is to make best use of these effects and to fully understand them in day-to-day information security.

## Converting Security Processes Into Security Subsystems

Security processes are often seen as linear: there is activity, a technical and organisational response, and subsequent observations of how things are changing. For instance, monitoring internal and external attacks is typically seen as an ongoing security process that involves organisational resources, technology and documentation of any issues arising. This is seen as linear because there are the initial attacks (or attempts), an immediate reaction, and logging and processing aspects. While this answers the question of *what* is happening—security breaches—it fails to explain *why* it is happening. To identify the underlying cause-and-effect relationships, each security process needs to be seen in a circular (systemic) way. **Figure 37** illustrates this for the example of internal attacks and what is behind them.



The circular representation effectively creates security subsystems that are more easily analysed and understood. As one step in this example leads to another, the number of total attacks is influenced by several external criteria—number of attackers and the availability of convenient exploits or attack vectors. However, the enterprise will respond systemically: attacks detected are pointing to certain vulnerabilities that are identified. A higher number of vulnerabilities obviously leads to an increased attractiveness of an attack—as does the lack of monitoring or countermeasures. Once it is known that the enterprise is vulnerable from within, this may change the overall attractiveness as a target, and the overall probability of an attack will increase.

If this continues, the enterprise will be caught in a systemic loop of increasing attacks. In a linear model, many solutions might come to mind that would stop this. However, they would treat the symptoms rather than the root cause, which is the perceived attractiveness. To get out of the systemic loop, security management will have to clearly decrease attractiveness by whatever means. This can be achieved by investing in security measures that address one or more of the steps in the loop or in the external influence factors.

Similarly, circular subsystems need to be formed from the other security processes and solutions identified throughout the enterprise. In practice, most of these circles, with their dependencies, are already known to security practitioners. However, they are rarely formalised or documented. BMIS is a useful tool to identify and categorise this information based on existing security processes.

### ***Actions and Improvement Steps***

In any of the security subsystems identified and described, there are some points at which security managers can influence the circular loop. Some things are always given and cannot be changed in practice, such as the number of exploits known to be in existence or the number of employees who might have the skills to enact an internal attack. Similarly, it is very difficult to influence the number of external attempts at attacking the enterprise (but it is possible to influence their success rate). Other elements of the

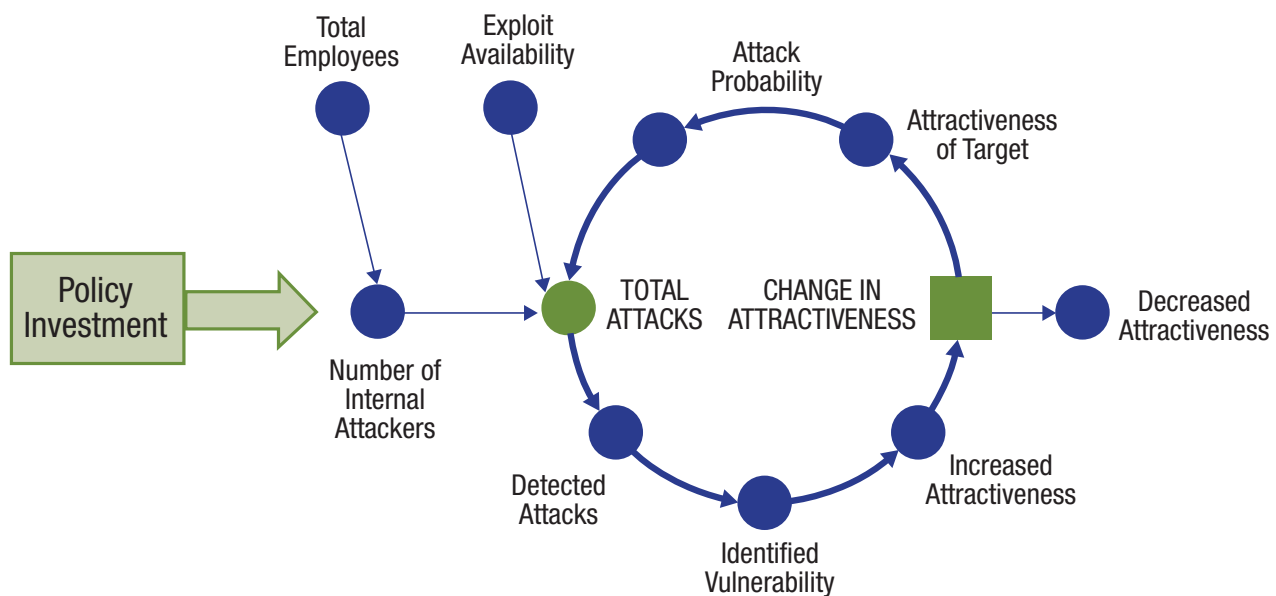
# THE BUSINESS MODEL FOR INFORMATION SECURITY

systemic loop are more accessible and may be improved by targeted investments and by strengthening security. The BMIS systemic view clearly highlights the leverage in each subsystem and the options available in terms of investing or introducing technical security measures.

**Figure 37** shows how the problem of internal attacks is addressed in a step-by-step manner using the available factors of influence in a gradual manner. For each action, there is a link back to the original structure of BMIS. This informs and enables the mapping back of actions taken to the tabular analysis of the current situation and the potential root causes, as described previously.

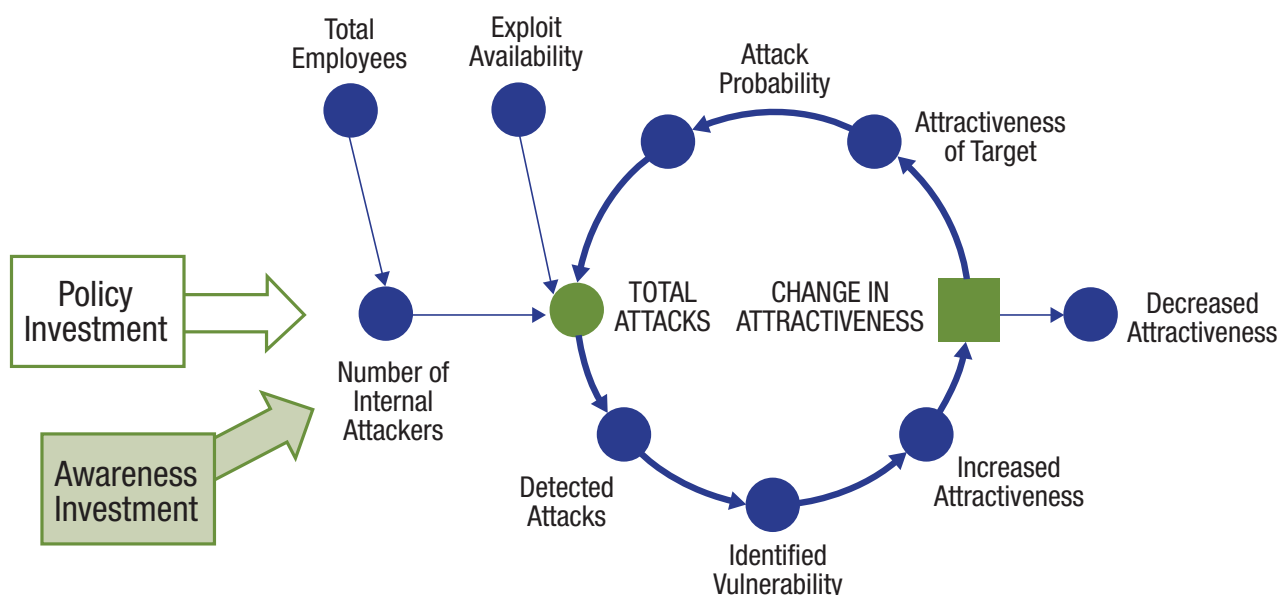
**Figure 38** shows what an investment in upgrading security policies might achieve. In terms of the model, the investment belongs to the Organisation element since it adds structure and governance to the overall information security system. In practice, investing in better policies would reduce the number of internal attackers, whereas reducing the number of available exploits (the other influencing factor) is rather difficult.

Figure 38—Investing in the Organisation Element



A singular investment in upgrading policies is unlikely to be sufficient to stop internal attacks. Therefore, the second step is to introduce awareness by investing in related programmes, as shown in **figure 39**. This does not change humans or organisational structures, so it is placed in the Culture DI of the model. After the first two steps in improving information security, both the Organisation element and the Culture DI have turned out to be useful targets for security investments.

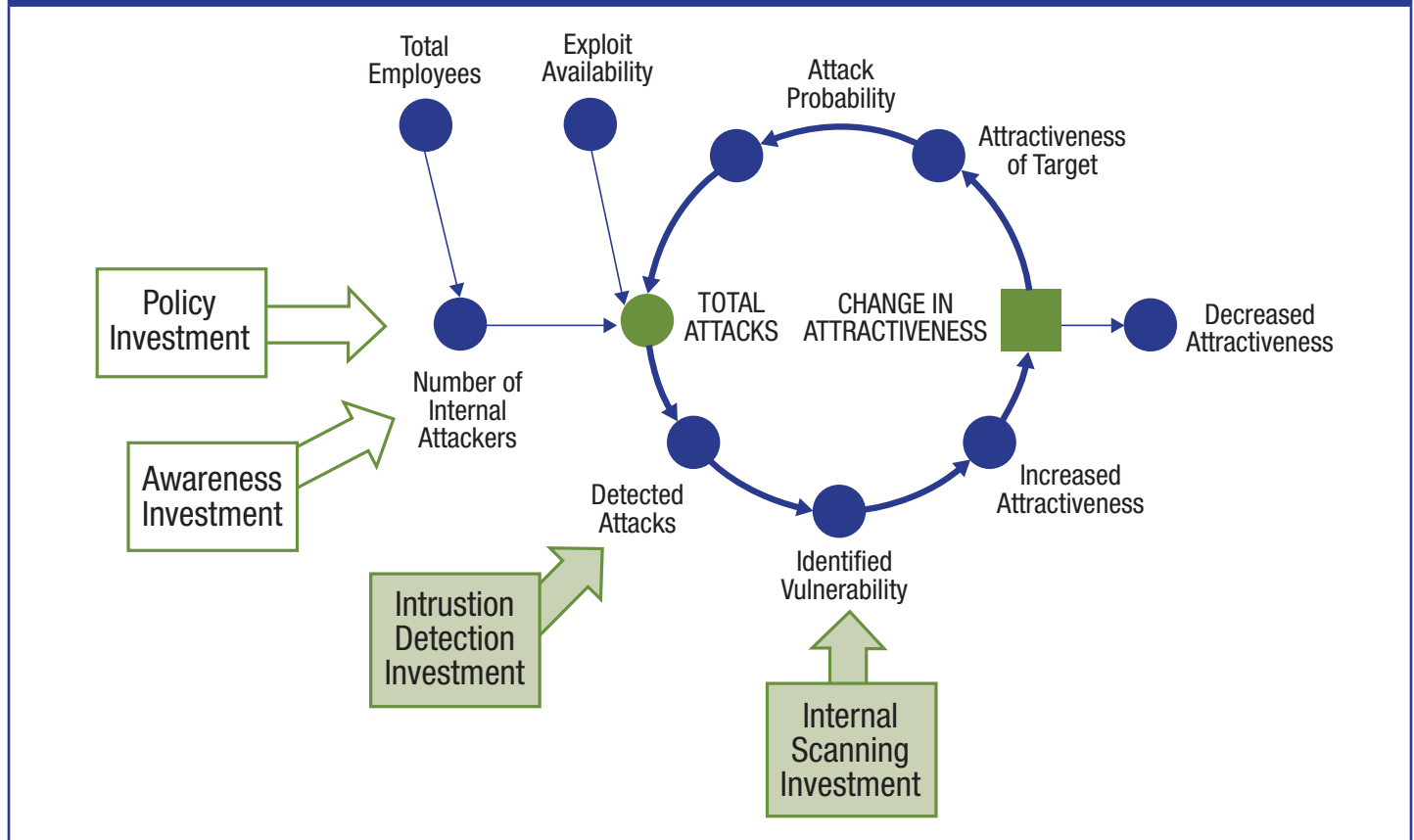
Figure 39—Investing in the Culture DI





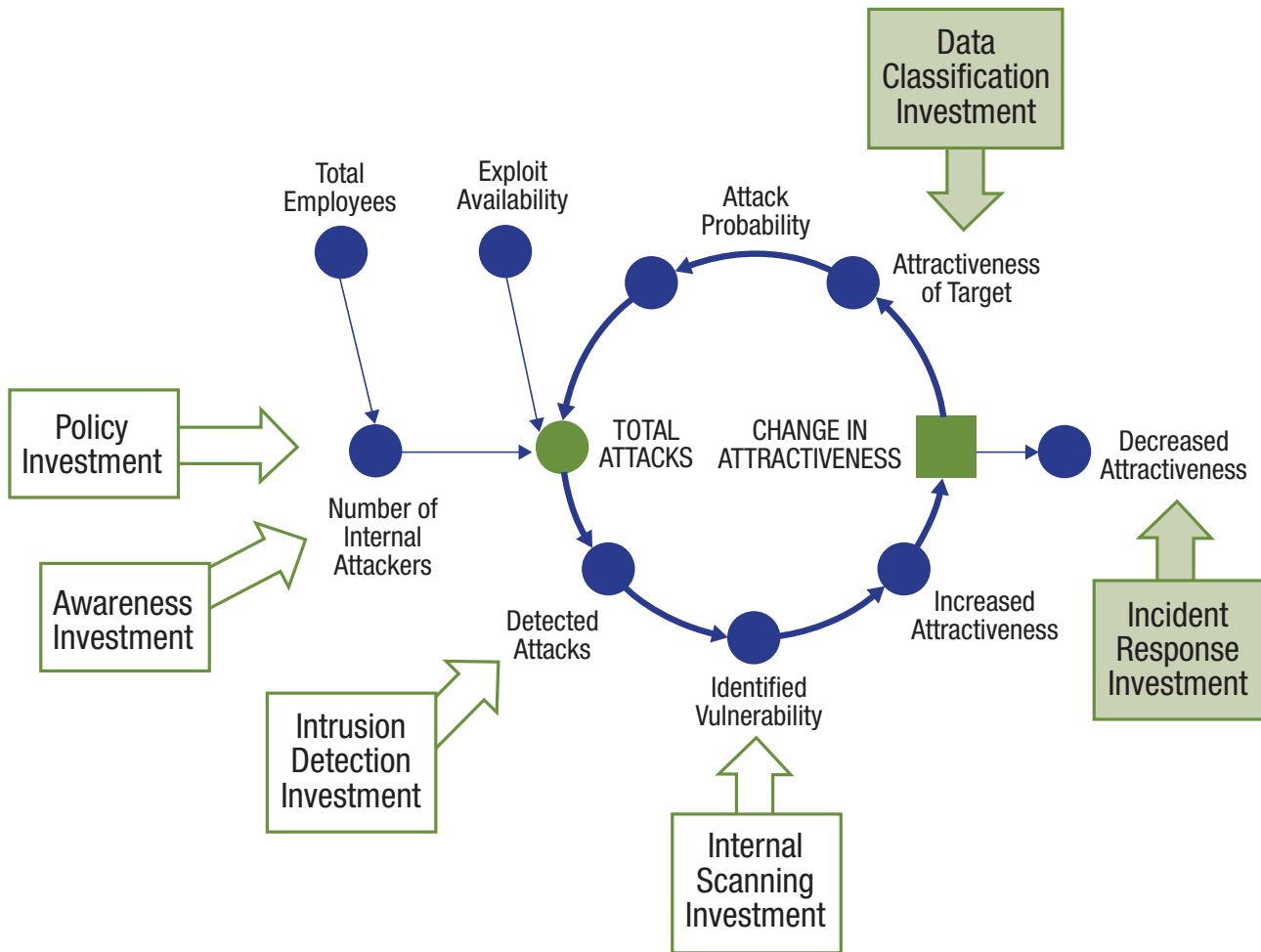
Inside the circular loop that determines the number of internal attacks, there are more points that allow interaction with the overall system, as shown in **figure 40**. The attack detection rate is an important defence against opportunistic or low-intensity attacks, and many perpetrators will think twice about attacking if the likelihood of being caught is high. An investment in intrusion detection, as part of the overall security architecture, will help in reducing the total number of attempted or successful attacks. In contrast to the policy and awareness investments, this action is designed to directly influence the systemic loop. Likewise, the investment in system- and application-level scanning for attacks focuses attention on what is happening inside the loop and reduces the number of existing vulnerabilities. In combination, both of these architectural security measures increase the level of protection within the system.

Figure 40—Investing in the Architecture DI



To complete the sequence of actions that are based on the circular model or subsystem for internal attacks, there are additional points of influence available. Incident response ensures that detected attacks are treated in the appropriate manner, thus increasing the risk for attackers. Similarly, classifying and securing data decrease the overall attractiveness of the target. Because these steps require process modifications, they are located within the Process element of the model (**figure 41**).

Figure 41—Investing in the Process Element



## Leveraging System Dynamics

Any system, whether simple or complex, will react to changes from the inside and outside. The system will either feed back or feed forward, depending on the circular dependencies, as shown in the previous example. This behaviour can be utilised to improve overall security and to leverage the self-reinforcing nature of many systems. Instead of using a simple ‘more of the same’ approach, as is often the case in practical information security, the systems approach will show very early in the process whether new security measures are actually improvements. As a first step, the broad suggestions for improving the situation in terms of internal attacks can be brought back to a tabular format to manage them in day-to-day business, as shown in **figure 42**.

**Figure 42** gives an overview of what needs to be done at a high level to reduce the number of internal attacks. The various investments are now broken down into manageable components by linking them to known governance, risk and compliance frameworks. As an example, they are mapped to COBIT in **figure 43**.

Figure 43—High-level Security Measures and COBIT

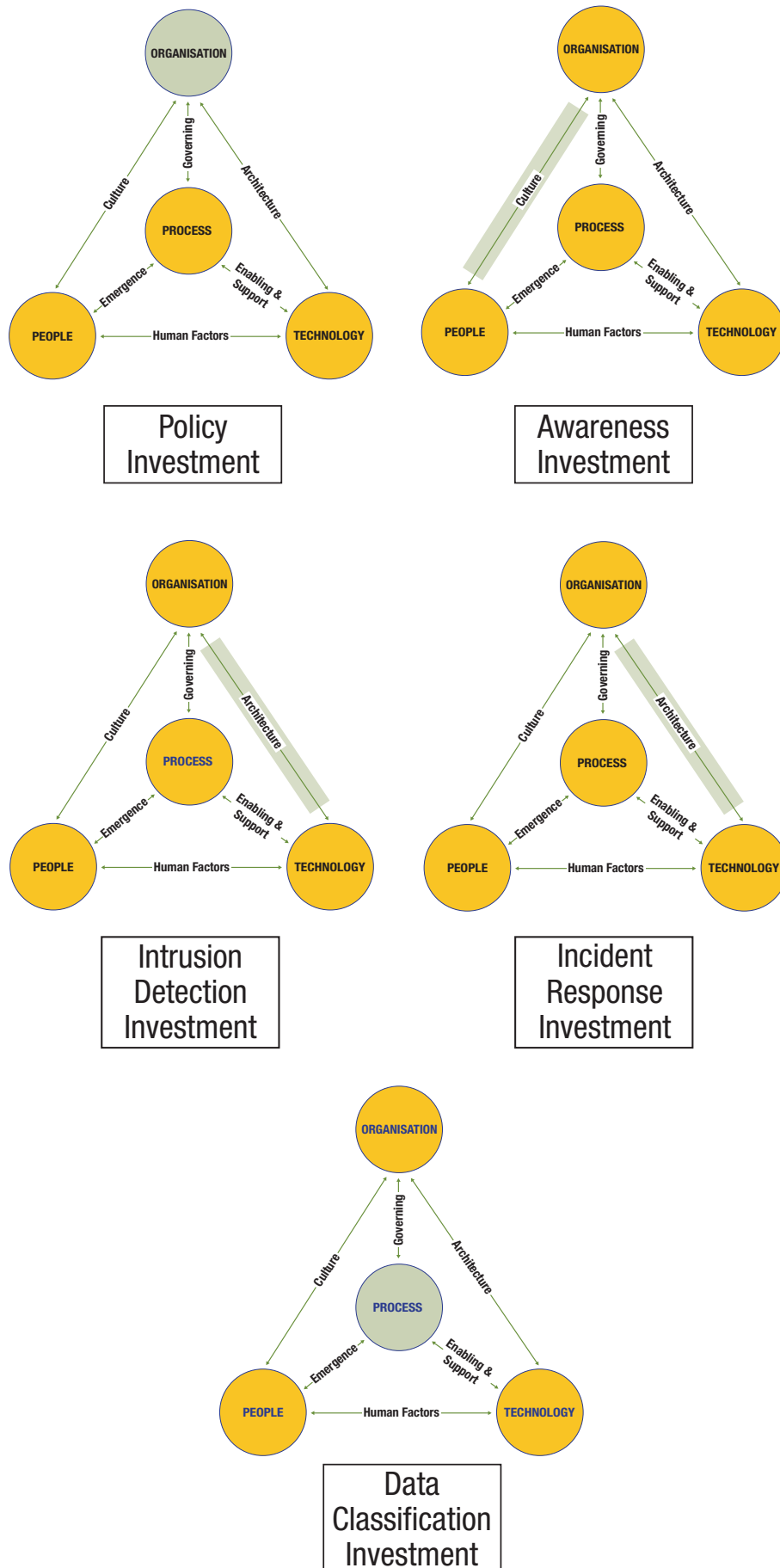
Security Investment/Improvement	COBIT Links
Policy investment	P01, P04, P06, P08, P09, DS5, DS7, ME4
Awareness investment	P06, P07, DS7, ME4
Intrusion detection investment	P02, P03, AI3, AI4, AI7, DS5, DS9, DS13
Incident response investment	P07, P09, DS8, DS10, ME2
Data classification investment	P02, P09, DS3, DS5, DS11

Depending on the situation and the overall IT goals of the enterprise, COBIT components may be applied in different ways, but all of the elements need to be considered when subdividing the investment into manageable steps and solutions. Mapping the general ideas and concepts in information security to the COBIT framework further ensures that the existing environment of risk, compliance and governance of IT is recognised and built in to the security programme.

### Conclusion

As security professionals continue to be faced with evolving challenges, examining new solutions to information security issues is necessary. Understanding BMIS and systems thinking in relation to information security programmes can be beneficial to anyone who needs to manage information security risk. ISACA will develop additional research reports that explore the DIs and their impact on information security programme performance. Additionally, practical guidance focusing on using the model in different scenarios will be offered. BMIS will also serve as a foundation for the upcoming COBIT security framework.

Figure 42—High-level Security Measures



## ISACA PROFESSIONAL GUIDANCE PUBLICATIONS

Many ISACA publications contain detailed assessment questionnaires and work programmes. Please visit [www.isaca.org/bookstore](http://www.isaca.org/bookstore) or e-mail [bookstore@isaca.org](mailto:bookstore@isaca.org) for more information.

### Frameworks and Models

- *The Business Model for Information Security*, 2010
- COBIT® 4.1, 2007
- *Enterprise Value: Governance of IT Investments, The Val IT™ Framework 2.0*, 2008
- *ITAF™: A Professional Practices Framework for IT Assurance*, 2008
- *The Risk IT Framework*, 2009

### BMIS-related Publications

- *Introduction to The Business Model for Information Security*, 2009

### COBIT-related Publications

- *Aligning COBIT® 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit*, 2008
- *Building the Business Case for COBIT® and Val IT™: Executive Briefing*, 2009
- *COBIT® and Application Controls*, 2009
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2<sup>nd</sup> Edition*, 2007
- *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*, 2007
- *COBIT® Mapping: Mapping of FFIEC With COBIT® 4.1*, 2007
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2<sup>nd</sup> Edition*, 2006
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*, 2007
- *COBIT® Mapping: Mapping of ITIL V3 With COBIT® 4.1*, 2008
- *COBIT® Mapping: Mapping of NIST SP 800-53 With COBIT® 4.1*, 2007
- *COBIT® Mapping: Mapping of PMBOK® With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of SEI's CMM® for Software With COBIT® 4.0*, 2006
- *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*, 2007
- *COBIT® Mapping: Overview of International IT Guidance, 2<sup>nd</sup> Edition*, 2006
- *COBIT® Quickstart™, 2<sup>nd</sup> Edition*, 2007
- *COBIT® Security Baseline™, 2<sup>nd</sup> Edition*, 2007
- *COBIT® User Guide for Service Managers*, 2009
- *Implementing and Continually Improving IT Governance*, 2009
- *IT Assurance Guide: Using COBIT®*, 2007
- *IT Control Objectives for Basel II*, 2007
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2<sup>nd</sup> Edition*, 2006
- *ITGI Enables ISO/IEC 38500:2008 Adoption*, 2009
- *SharePoint® Deployment and Governance Using COBIT® 4.1: A Practical Approach*, 2010

### Risk IT-related Publication

- *The Risk IT Practitioner Guide*, 2009

### Val IT-related Publications

- *The Business Case: Using Val IT™ 2.0*, 2010
- *Enterprise Value: Getting Started With Value Management*, 2008
- *Value Management Guidance for Assurance Professionals: Using Val IT™ 2.0*, 2010

### Executive and Management Guidance

- *An Executive View of IT Governance*, 2008
- *An Introduction to The Business Model for Information Security*, 2009
- *Board Briefing on IT Governance, 2<sup>nd</sup> Edition*, 2003
- *Defining Information Security Management Position Requirements: Guidance for Executives and Managers*, 2008
- *Identifying and Aligning Business Goals and IT Goals: Full Research Report*, 2008
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2<sup>nd</sup> Edition*, 2006

## Executive and Management Guidance (cont.)

- *Information Security Governance: Guidance for Information Security Managers*, 2008
- *Information Security Governance—Top Actions for Security Managers*, 2005
- *IT Governance and Process Maturity*, 2008
- IT Governance Domain Practices and Competencies:
  - *Governance of Outsourcing*, 2005
  - *Information Risks: Whose Business Are They?*, 2005
  - *IT Alignment: Who Is in Charge?*, 2005
  - *Measuring and Demonstrating the Value of IT*, 2005
  - *Optimising Value Creation From IT Investments*, 2005
- IT Governance Roundtables:
  - *Defining IT Governance*, 2008
  - *IT Staffing Challenges*, 2008
  - *Unlocking Value*, 2009
  - *Value Delivery*, 2008
- *Managing Information Integrity: Security, Control and Audit Issues*, 2004
- *Understanding How Business Goals Drive IT Goals*, 2008
- *Unlocking Value: An Executive Primer on the Critical Role of IT Governance*, 2008

## Practitioner Guidance

- Audit/Assurance Programs:
  - *Change Management Audit/Assurance Program*, 2009
  - *Cloud Computing Audit/Assurance Program*, 2010
  - *Crisis Management Audit/Assurance Program*, 2010
  - *Generic Application Audit/Assurance Program*, 2009
  - *Identity Management Audit/Assurance Program*, 2009
  - *Information Security Management Audit/Assurance Program*, 2010
  - *IT Continuity Planning Audit/Assurance Program*, 2009
  - *Network Perimeter Security Audit/Assurance Program*, 2009
  - *Outsourced IT Environments Audit/Assurance Program*, 2009
  - *Securing Mobile Devices Audit/Assurance Program*, 2010
  - *Security Incident Management Audit/Assurance Program*, 2009
  - *Systems Development and Project Management Audit/Assurance Program*, 2009
  - *UNIX/LINUX Operating System Security Audit/Assurance Program*, 2009
  - *Windows Active Directory Audit/Assurance Program*, 2010
  - *z/OS Security Audit/Assurance Program*, 2009
- *Cybercrime: Incident Response and Digital Forensics*, 2005
- *Enterprise Identity Management: Managing Secure and Controllable Access in the Extended Enterprise Environment*, 2004
- *Information Security Career Progression Survey Results*, 2008
- *Information Security Harmonisation—Classification of Global Guidance*, 2005
- *OS/390—z/OS: Security, Control and Audit Features*, 2003
- *Peer-to-peer Networking Security and Control*, 2003
- *Risks of Customer Relationship Management: A Security, Control and Audit Approach*, 2003
- *Security Awareness: Best Practices to Serve Your Enterprise*, 2005
- *Security Critical Issues*, 2005
- *Security Provisioning: Managing Access in Extended Enterprises*, 2002
- *Stepping Through the InfoSec Program*, 2007
- *Stepping Through the IS Audit*, 2<sup>nd</sup> Edition, 2004
- Technical and Risk Management Reference Series:
  - *Security, Audit and Control Features Oracle® Database*, 3<sup>rd</sup> Edition, 2009
  - *Security, Audit and Control Features Oracle® E-Business Suite*, 3<sup>rd</sup> Edition, 2010
  - *Security, Audit and Control Features PeopleSoft*, 2<sup>nd</sup> Edition, 2006
  - *Security, Audit and Control Features SAP® ERP*, 3<sup>rd</sup> Edition, 2009
- *Top Business/Technology Survey Results*, 2008
- White Papers:
  - *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspective*, 2009
  - *New Service Auditor Standard: A User Entity Perspective*, 2010
  - *Securing Mobile Devices*, 2010
  - *Social Media: Business Benefits and Security, Governance and Assurance Perspectives*, 2010





**Page intentionally left blank**

**Page intentionally left blank**



3701 Algonquin Road, Suite 1010  
Rolling Meadows, IL 60008 USA  
Phone: +1.847.253.1545  
Fax: +1.847.253.1443  
E-mail: [info@isaca.org](mailto:info@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)

